EiS Kent Lightspeed Mobile Device Management (MDM) User Guide

20 May 2013

CONTENTS

MDM PREFACE **4**

MDM NAVIGATION **5**

MDM Dashboard 5
Global Menu *5*
Group Level Menu *6*
Breadcrumbs *7*
Pen and Link *7*
Profiles, Apps and + ... *8*

MDM ADMINISTRATORS **9**

Create Administrators *10*
Create Delegated Administrators *10*
Delete an Administrator or Delegated Administrator *11*

MDM OBJECT STRUCTURE **12**

Inheritance 12

MDM GROUPS **14**

Planning a Group hierarchy 14
Creating a Group 15
Group Types *16*
Delete a Group *17*
Users 18
Assign User to a Group *18*
Remove User from a Group *19*
Edit/viewing User Information *19*
Devices 21
Remove Device from a Group *22*
Remove Device from a User *23*
Device Property Page *24*

MDM PROFILES **25**

Profile Navigation *25*
Profile Variables *26*

MDM APPS **28**

View School Level Apps *28*
View Group level Apps *29*
Install an App 30
Web App Install *30*
iTune App Install *32*

ENROLMENT **33**

Apple Configurator and Apple Supervise Mode 33
Using Apple Configurator *34*
Device Enrolment 38
Bulk Enrolment *39*
Individual Enrolment *40*
Advanced Enrolment options 42
Authenticating Devices to Users (Individual Enrolment) *42*

APPLE INFORMATION **44**

Apple Deployment Options 44
Apple Education Volume Purchase Programme 45
Apple ID/iTunes Accounts 46

MISCELLANEOUS INFORMATION **47**

Where do I begin? 47
How Do I…? 48
My Apple VPP spreadsheet *49*

TROUBLESHOOTING **51**

MDM REFERENCE SHEET **52**

MDM PREFACE

This MDM User Guide has been written primarily to help advise and guide EiS Schools Broadband connected schools in using Lightspeed's Mobile Device Manager (MDM) and optimizing it for their use within their schools network and day to day activities however, it will also be of interest and use to non EiS Schools Broadband customers too.

Lightspeed MDM is a cloud based Mobile Device Manager tool, accessible 24/7 from any location via an internet URL and requires no MDM server be installed onsite at the school. This allows you to hierarchically manage your schools mobile and tablet devices remotely wherever they are in the world providing that the devices have an internet connection. Mobile and tablet technology is evolving at a rapid rate and Lightspeed MDM strives to match these developments to keep up to date with all the features and functionality that is being added to the devices by their vendors. This means that new features will be automatically added to MDM from time to time together with support for other platforms such as Android, Win 8 and OSX mobile devices. This guide is currently written with only Apple iOS devices such as iPads and iPhones in mind but will be updated as the other OS's become available.

It will help explain some common concepts throughout MDM such as hierarchical MDM Groups and how they may be used to help organise your schools devices into common groups such as Staff devices and Student devices and discusses how you may wish to further granulise this if you require different levels of Staff or Student devices, perhaps based on curricular subject or age groups.

It also demonstrates how to use Apples Supervise Mode to ensure that you have greater control over your Apple iOS devices (typically iPads and iPhones) and the importance of implementing this Supervise Mode from the outset before using MDM to manage those devices. There is a pictorial walkthrough how to accomplish this coupled with the use of Bulk Enrolment, the MDM process that its anticipated most schools would be using to put their devices into MDM management.

For Apple newcomers we have also included a section that we hope demystifies and helps remove some of the perhaps confusing terminology that Apple requires a school to know in order to optimise their schools future Apple experience. This provides guidance on how, where and why a school would benefit from registering online for Apples Volume Licensing Programme for App and content purchases in order to retaining ownership of the purchases. It also provides some guidance on how to use Apples iTunes in order to make those purchases and then how to deploy them through MDM.

We hope that you find this guide very useful and look forward to hearing any feedback so that we may amend or clarify any information as appropriate.

MDM NAVIGATION

To login to Lightspeed MDM please navigate in a browser to: - https://www.lsmdm.com

You will then need to authenticate using your Administrator email address and password.

MDM Dashboard

After authenticating into MDM you will land on a screen much like below, this will be the root folder for your school ("A Big School – 0000" will be replaced by your schools name).

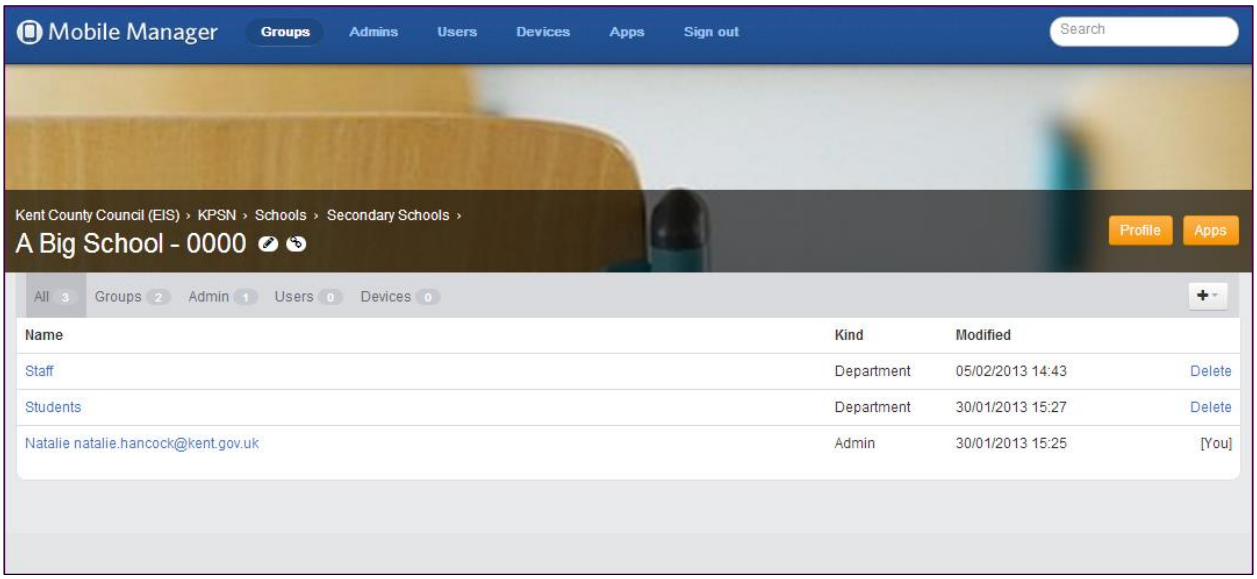


Fig 1.01

From this root page you will see any Groups, Administrators, Devices or Users that you may have assigned to this Group. The same principal will apply to subsequent Groups as you navigate up the tree (i.e., Staff and Students in the above).

Global Menu

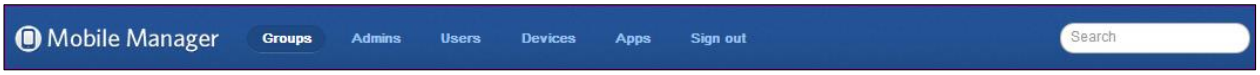


Fig 1.02

Clicking this School Menu on Groups, Admins, Users, Devices and Apps will take you to the Root level and list the items accordingly. For example, if you click on Devices then you would see ALL the devices that are registered for your school.

Group Level Menu

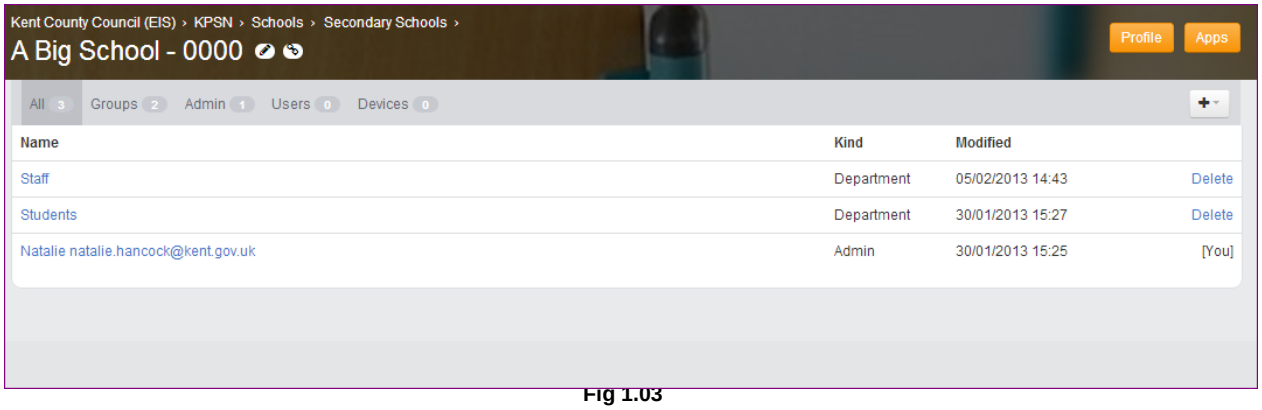


Fig 1.03

This menu allows you to view the items that belong to the Group that you are currently within, for example, in the above you are in “A Big School – 0000”, clicking on Groups would display ALL the Groups contained in the Root Group only (removing other items).

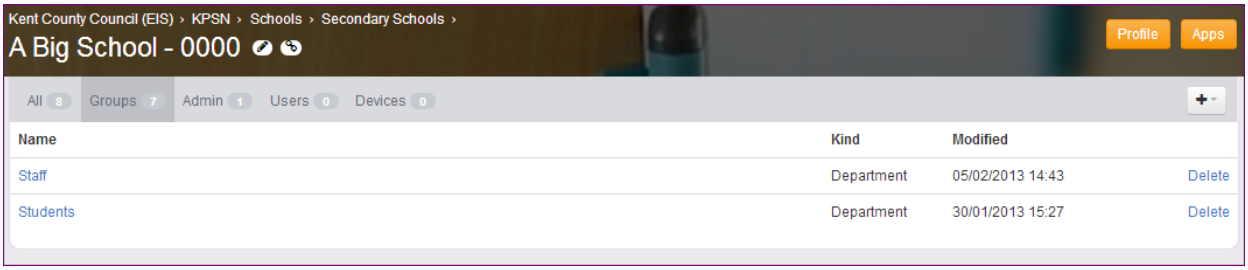


Fig 1.04

Click Admin.

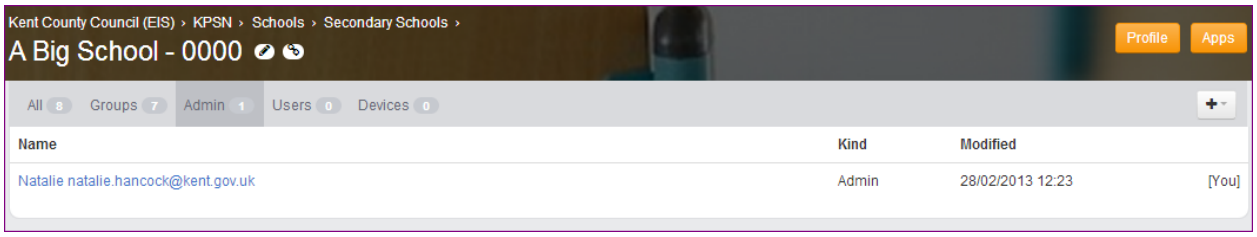


Fig 1.05

These Group level filters could be useful for removing extraneous information from view when the Group might contain User, Devices, Administrators and other Groups. This is a viewing option only; the filtered information is not deleted!

Breadcrumbs

As you navigate around your Group structure you may move backwards through your structure by clicking on your breadcrumbs, located here.

Fig 1.06

The above shows that you are currently within a Group called IT Techs, a glance along the breadcrumb trail advises you that you are currently underneath Staff which is itself beneath the Root.

Fig 1.07

Simply click on either Group if you wished to jump straight up to that level, for example, clicking on Staff takes you up one level (Note that you will see IT Techs within the Group window once again.

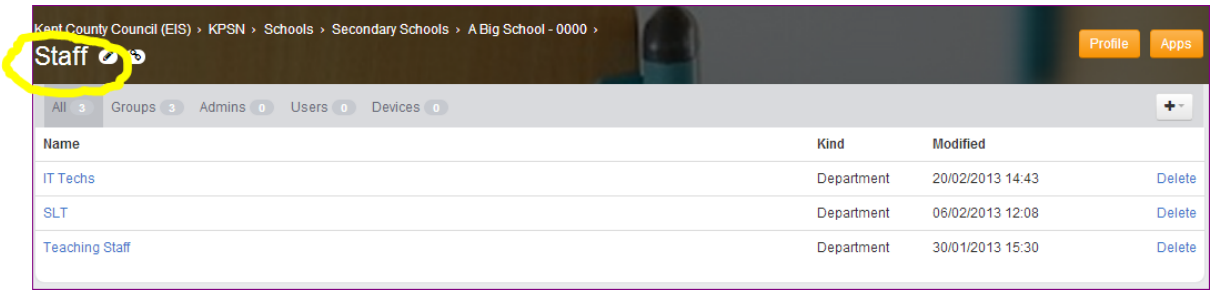


Fig 1.08

Pen and Link

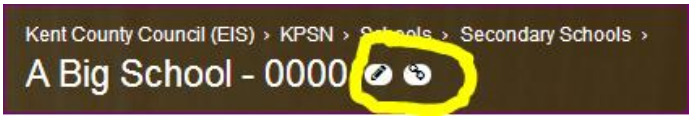


Fig 1.09

The leftmost pen symbol (Fig 1.09) allows you to edit the current level's Details (Fig 1.10).

The rightmost chain symbol (within circled) is the link that you would need for enrolling devices into this Group (Bulk or Individual Enrolment).

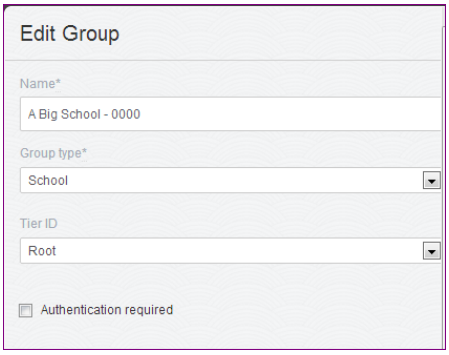


Fig 1.10

Profiles, Apps and +

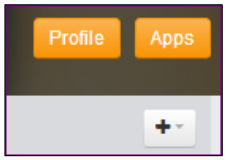


Fig 1.11

Clicking on Profile allows you to configure the profile options that are to apply to members of that Group; these will be applied in live time to all devices that belong to that Group (See Profile for further information)

Click on Apps to deploy Apps to the devices in that Group. This will allow you to Upload an App or to browse the iTunes App Store, redeem VPP codes etc. (See Apps for further information).

Click on + (Fig 1.12) to reveal further available options.

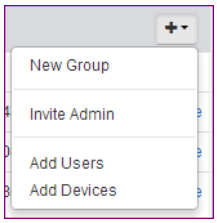


Fig 1.12

New Group creates a New Group folder from this point (See Groups for further information).

Invite Admin allows you to enter an email address of someone that you wish to set up as an Administrator or Delegated Administrator (if not on the Root). (See Administrators for further information).

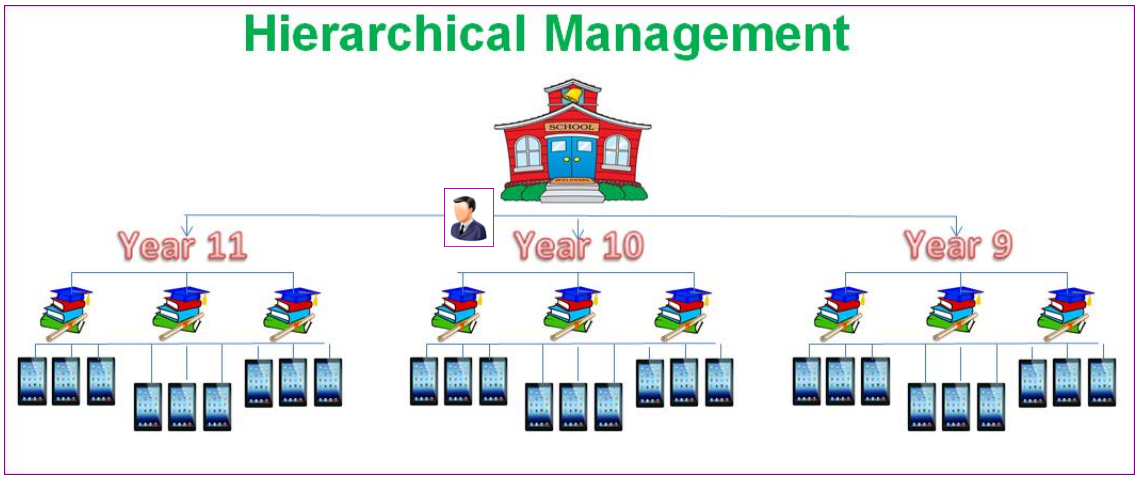
Add User allows you to assign an AD User into a Group. (See Users for further information).

Add Device allows you to assign existing devices to a User. (See Devices for further information).

MDM ADMINISTRATORS

Administrators in MDM are roles that are responsible for managing your schools Group structure and environment. It may be that the main Administrator creates your Group structure and enrols the devices into MDM, managing what may be considered your schools infrastructure; however, they may not be the ones to manage the individual devices.

Delegated Administrators may be created at the level of each Group; these Delegated Administrators would then manage all the objects that reside below them. For example:



.

Fig 2.01

In the above you have the Administrator ( ) at the root, however, as in the below, you could create a Delegated Administrator at each of the three Year # levels. They would then be able to manage the objects within their respective Year # Groups only, whilst the Root Administrator can manage all three.

Fig 2.02

You may wish to introduce further Delegated Administrators organised by clubs or curricular subject but the hierarchical model above serves to illustrate how the Delegated Administrator role may be useful for you.

Create Administrators

To create additional Root Administrator accounts for your colleagues please click on the + symbol on the right of your landing page, for example;

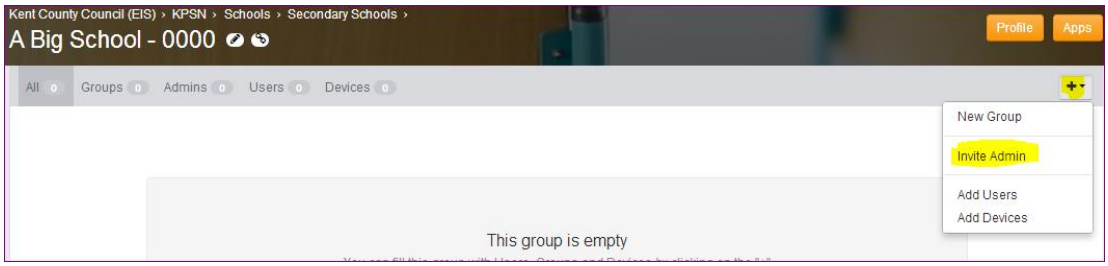


Fig 2.03

And select “Invite Admin” (highlighted above)

Populate the Email* field with a valid school email address and select “Send invitation”

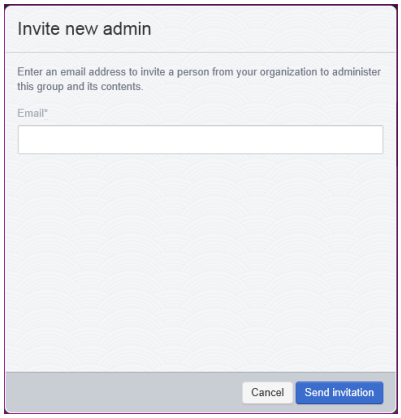

Invite new admin
Enter an email address to invite a person from your organization to administer this group and its contents.
Email*
Cancel
Send invitation

Fig 2.04

Your colleague will receive an invitation a few moments later from Lightspeed (support@lightspeedsystems.com) inviting them to verify the account and to set a password. If it is not received within 15 minutes please verify that it is not in a Spam or Junk folder.

Create Delegated Administrators

To create a Delegated Administrator you will need to navigate to the lowest Group that you wish them to manage from and click on the + symbol on the right of the desired groups landing page and then simply follow the same instructions as for a Root Administrator.

The below (Fig 2.05) creates a Delegated Administrator in a Group called Year 13 (Year 13 exists within another Group called Students).

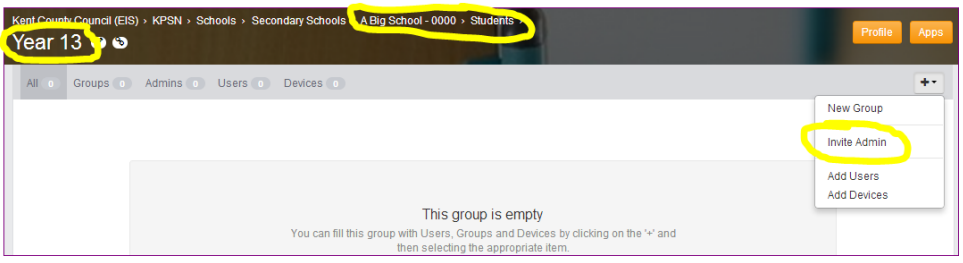

Kent County Council (EIS) › KPSN › Schools › Secondary Schools › A Big School - 0000 › Students ›
Year 13
Profile
Apps
All
Groups
Admins
Users
Devices
New Group
Invite Admin
Add Users
Add Devices
This group is empty
You can fill this group with Users, Groups and Devices by clicking on the '+' and then selecting the appropriate item.

Fig 2.05

Delete an Administrator or Delegated Administrator

If you should need to remove an Administrator (Delegated or root) then simply navigate to the appropriate folder or select Admins from the Organisation Bar at the top and then select “Delete” against the entries that you wish to remove, i.e.

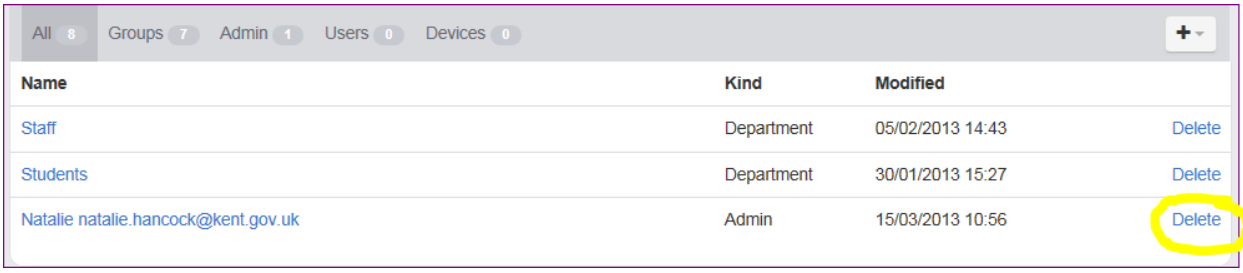


Fig 2.06

MDM OBJECT STRUCTURE

Inheritance

Lightspeed's MDM organisational structure is comprised of Groups, Devices and Users and consequently, as a result of the potential for nesting, that is that a Device could belong to a User who is themselves a member of a Group, MDM needs a way to determine which profile it is to ultimately apply to the object (Group, User or Device). To achieve this MDM has a hierarchy of what object type (Group, User or Device) inherits which settings from what parent object.

Devices can only be in one Group at a time. If, for example, as shown in the picture below (Fig 3.01), a device is in Group F then it would inherit settings from Groups C and A.

Users can exist in many groups. Users inherit apps and policies as follows:

- If a user is in two groups on the same inheritance branch then they get the lowest/deepest policy
- If a user is in two groups then the device would receive both profiles. For example, if the User is in both groups B and C as shown in Fig 3.01 then the device would have profiles from both Groups applied

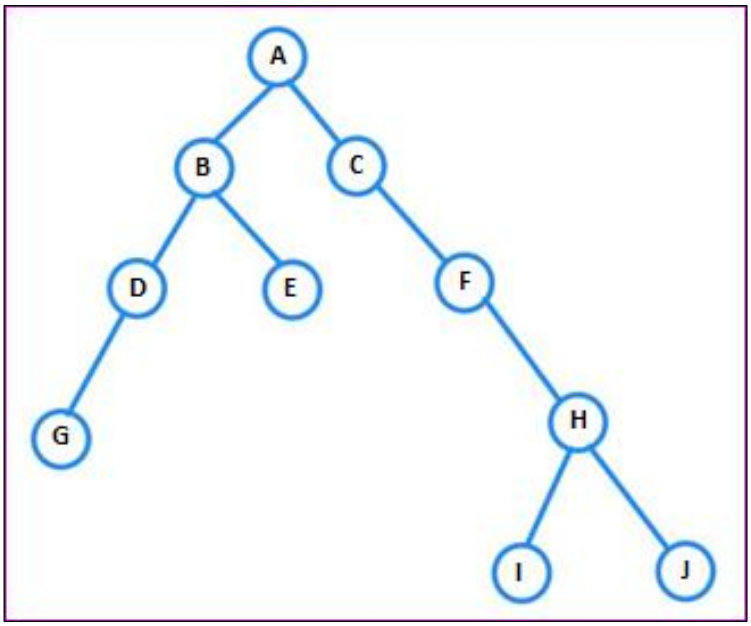


Fig 3.01

To illustrate with some example, using the picture above (Fig 3.01)

- A is your school
- If a user with a device is in Groups C and H then the device would receive a profile from Group H since it is lower on the Organisation tree
- If a user with a device is in Groups B and C then the device will receive the most restrictive profile
- If a user with a device is in Groups B, E, F, and J then they would receive profiles from both E and J since they are lowest on the tree on their respective organisational membership branches

Important to Note – For safety, Conflict Resolution in MDM is always handled by the most restrictive action being applied

 © EiS Kent

MDM GROUPS

Lightspeed MDM uses Groups in much the same way as an OU (Organisational Unit) is used within Active Directory (AD) environments. Groups may contain Devices, Users, Administrators or other Groups and these objects may inherit settings from the Group above them or exclusively use a specific Profile created for that Group. This hierarchy is dependent on the type of object it is (Group, User or Device) and its membership around your schools overall Group structure. (Please see hierarchy for further information)

Each Group may have its own Profile assigned to it which will apply to all devices that are enrolled within it. This profile may contain what functions are to be Enabled/Disabled on the device, mail settings, Restrictions (such as preventing Apps being installed, use of the Internet), enforcement of Passcode, etc. (Please see Profiles for further information).

Planning a Group hierarchy

It is advisable to spend a bit of time thinking about how you would like to manage your enrolled devices as the group structure within Lightspeed MDM is hierarchical. This means that if you make a change to the devices at the Root (School) level then it will recurse to ALL devices underneath the Root (with the exception of any groups that have the School Type assigned to them (see Type for further clarification)). If you make a change to a Group folder that may be 5 steps down from the Root then it will only affect the devices from that point downwards, i.e., the first 4 levels will be untouched.

We envisage that most schools would want to manage their Staff and Student devices independently of each other, for example, if Camera is disabled for Student devices it may still be desirable to keep the service Enabled on the Staff devices. Therefore, a typical starting point may look like;

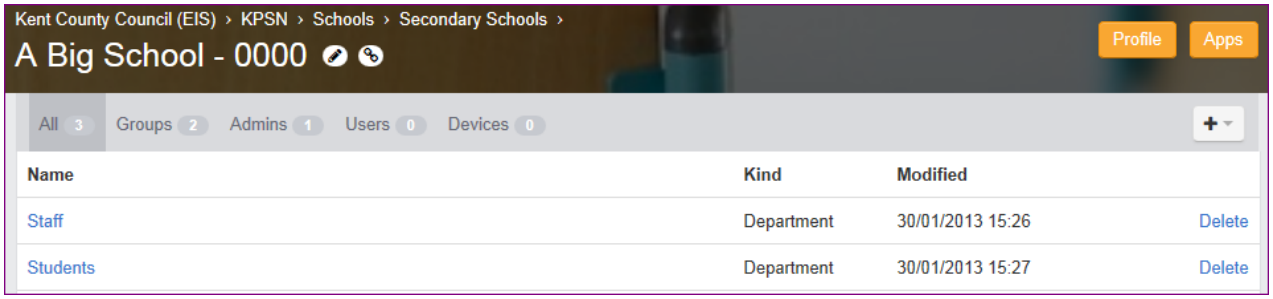


Fig 4.01

In the Staff (Fig 4.01) you may wish to create additional granularity of profiles by then creating additional containers, such as.

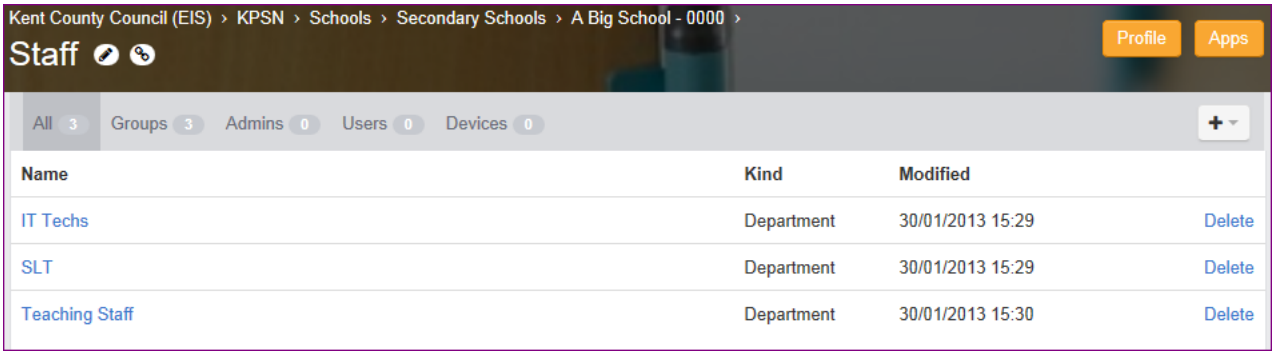


Fig 4.02

This would mean that you could enrol your devices into the appropriate Groups and then affect each Group either independently (so that they may have separate profiles of Apps and Restrictions) or from its respective Parent Group (so that all Child Groups are receive a common profile of Apps and Restrictions). For example, in the above case (Fig 4.02) a device in the SLT Group would not be affected by changes to the Teaching Staff or IT Techs Group however, any changes made to the parent Staff Group would affect ALL devices contained within IT Techs, SLT and Teaching Staff.

Creating a Group

Firstly you will need to navigate to the Group that you require you're new Group to belong to and click on + then select New Group.

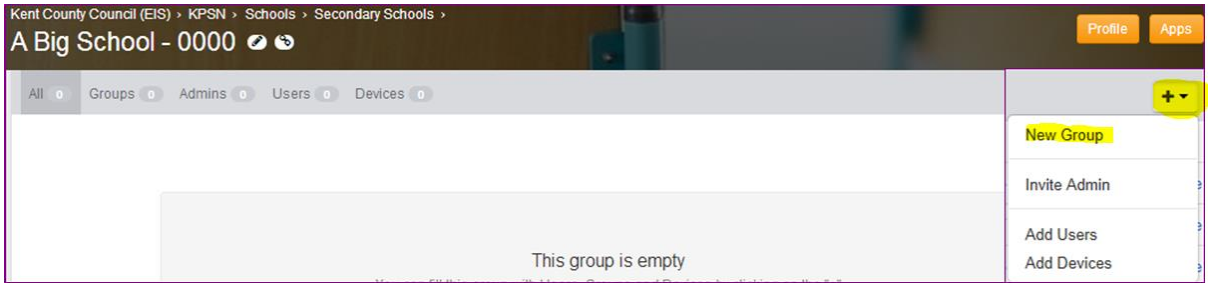
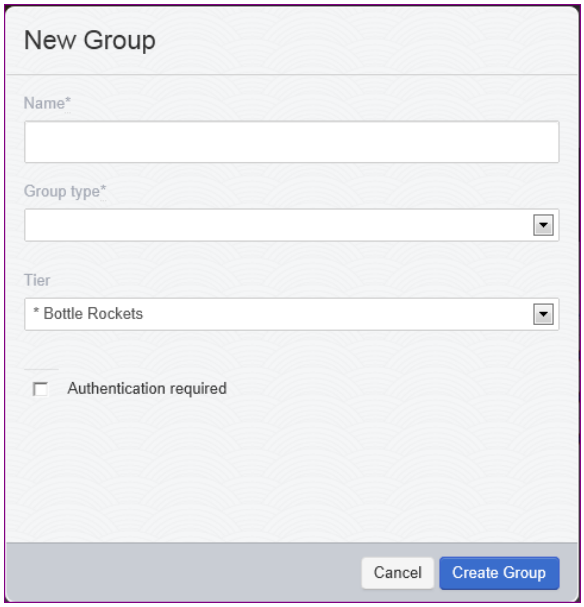


Fig 4.03

Complete details for the new Group.



Mandatory fields

Name * - This will be the group name

Group type * - School, Department, Cart, Class, Club

Group Types

With the exception of the School Type, these are simply labels and may be used to visually identify the type of category that a Group of devices belong to, such as an after school club, a particular Class or Department within your school. Department will be suitable for most scenarios.

School is a special Type classification which might be used in situations where more than one school may exist as a customer, share local IT Support and wish to organise their Lightspeed MDM structures in one Group. School classification also applies a boundary to the upper hierarchy so that its Child Groups will remain untouched by the Parent Group above itself. For example, in the screenshot below (Fig 4.05), the parent Group is Staff;

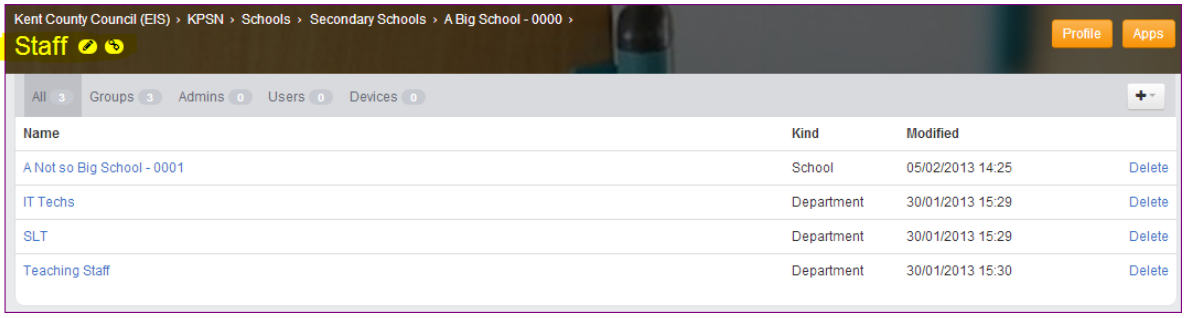


Fig 4.05

Any changes here will affect the Groups “IT Techs”, “SLT” and “Teaching Staff” but will not affect “A Not so Big School – 0001” or its Child Groups as its Type is defined as School.

Optional fields**

Tier – List of Next Gen Filtering Tiers

Authentication Required – (Yes / No) Default No

** Tier and Authentication

If you are asked to specify the "Tier" when creating your new Group and you are using our Lightspeed Next Gen for your schools Internet filtering and you require your devices to be authenticated against your schools DC prior to Individual Enrolment then please select your schools Next Gen Filtering tier from the dropdown list and tick "Authentication Required". (Please see Users or Authenticating Devices to Users for further information on assigning devices to Users).

If you do not require your devices to Authenticate against your schools DCs prior to individual Enrolment then ignore the Tier selection and ensure that "Authentication Required" remains unticked.

Delete a Group

If you should need to remove a Group then simply navigate to the appropriate parent Group and then select "Delete" against the entries that you wish to remove, for example, to remove the Staff Group.

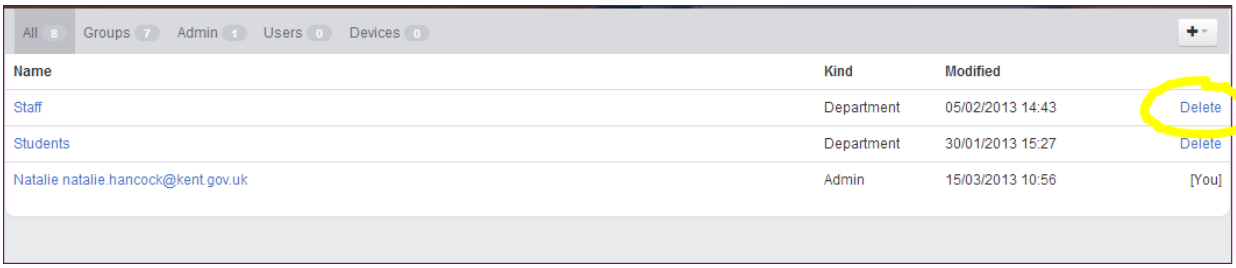


Fig 4.06

If you have any Devices remaining within that Group then any Group deployed Apps and Profile settings will also be removed. This won't remove Apps that have been installed outside of MDM.

Users

Users is an organisational object in MDM and will typically belong to a Group. A User would typically be assigned an iOS device such as an iPhone, iPad or iPod and you could see many Device objects to a User.

This could be useful in environments where you may have a mobile device per student or staff member and wish to integrate and configure the device with bespoke settings, such as configuring email, proxy etc.

You will only have access to manage Users if you have chosen to Enrol your devices using Forced Authentication. This process of integration creates an instance of the Authenticated User into MDM for you to then manage; you cannot create Users within MDM itself. (Please see Authenticating Devices to Users for further information on this Forced Authentication process).

Assign User to a Group

To assign an existing User to another Group (remembering that Users can exist in many Groups so you will need to remove from any unnecessary Groups) you will need to navigate to the intended Group that you wish the user to belong to.

Once at the desired Group

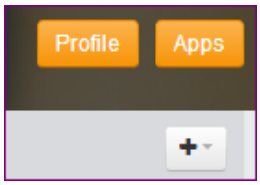


Fig 4.07

Select the Add symbol (Fig 4.07);

Select “Add User” from the drop down (Fig 4.08);

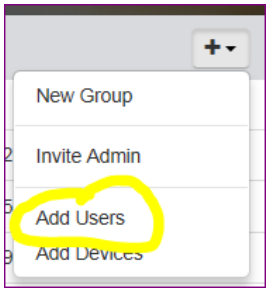


Fig 4.08

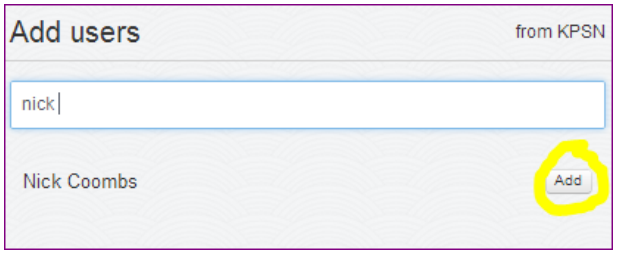


Fig 4.09

Enter the Username of the desired User and if it is recognised as a valid user it will appear below the search box (Fig 4.09).

Select Add (circled Fig 4.10) against the User that you wish to Assign to the Group, it will change to Added when done.

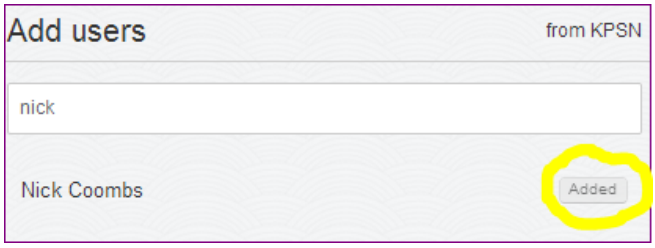


Fig 4.10

The User would now appear within that Group (Fig 4.11).

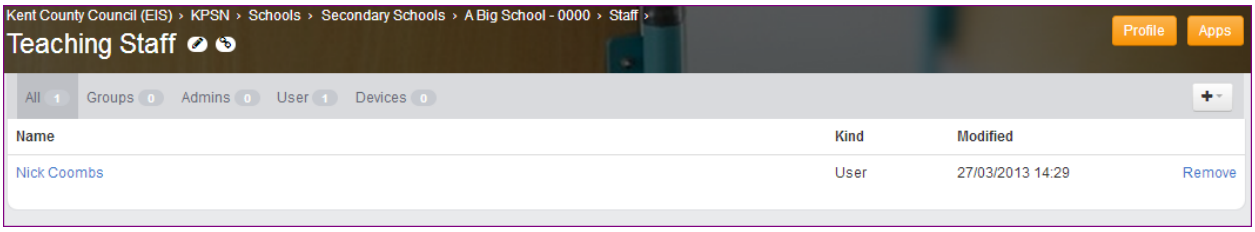


Fig 4.11

Remove User from a Group

To Remove a User from a Group you will need to navigate to the Group you wish to remove the User from and then select Remove next to their User instance, i.e.

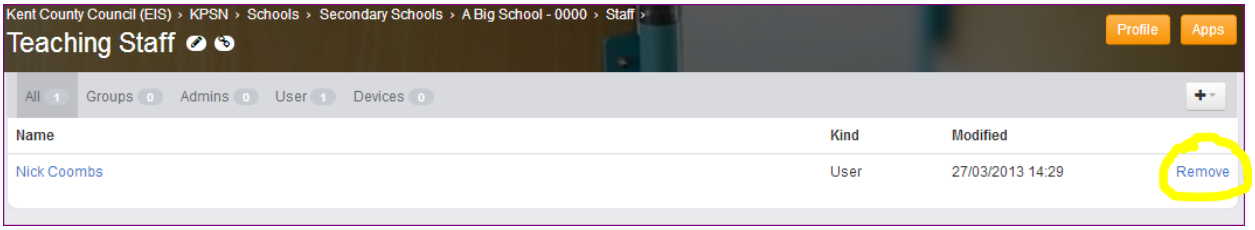


Fig 4.12

The above User would be removed from the Group “Teaching Staff” only, remaining in any other Groups accordingly.

Edit/viewing User Information

To view User based information (such as which Apps are installed, which Groups they belong to, which Profiles are installed, the LDAP path etc.) select the User instance. You can either navigate to the User within a specific Group or select Users from the School level menu.

Clicking on the User will reveal.

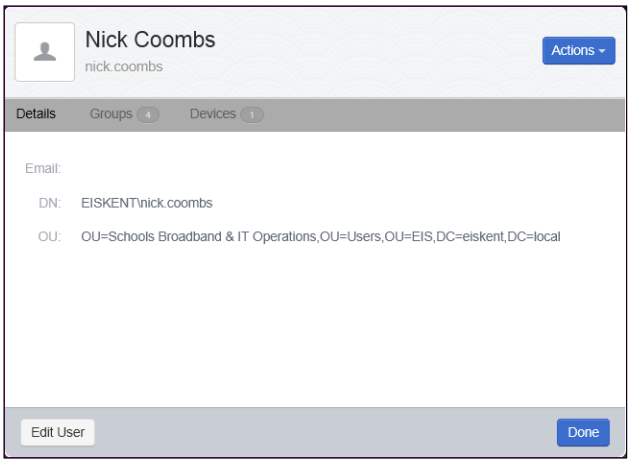


Fig 4.13

Click Edit User to correct or amend First name, Last name and email address
Click Done when finished with the User entry Window.

Groups states how many Groups the User is a member of, selecting this reveals those Groups (Fig 4.14).

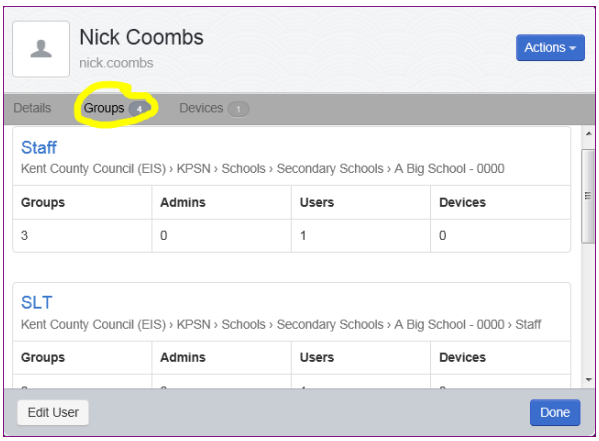


Fig 4.14

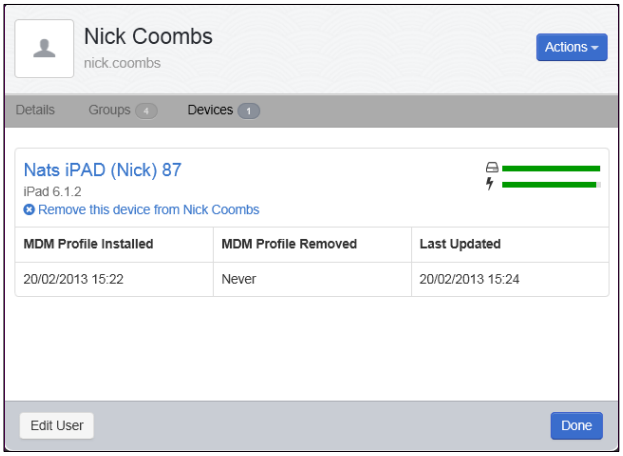


Fig 4.15

Devices states how many Devices the User has and selecting this reveals information about those Devices.

Actions allow you to search and Add devices to the user.

Devices

Device is an organisational object in MDM and will typically belong to a Group. A Device would typically be an iOS device such as an iPhone, iPad or iPod and you may see many Device objects per Group. You will only have access to manage Devices once you have enrolled them into MDM, you cannot create new Devices within MDM itself. Management might involve moving the Device from one Group to another; assign a Device to a registered User, editing the Asset Tag, viewing installed profiles or apps, wiping a lost device etc.

Assign a Device to a Group.

Important Note: - A Device can only exist in one Group at a time, this means that by assigning it to another Group then the current profile will be removed and the new Group Profile applied.

To assign a Device to an existing Group you should navigate to the intended Group.

Once in that Group select Add (Fig 4.16).

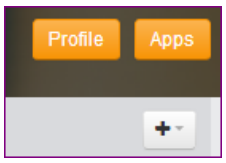


Fig 4.16

Then select “Add Device” (Fig 4.17).

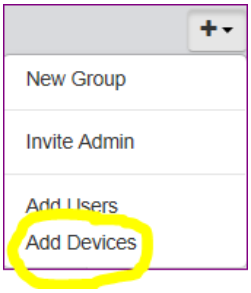


Fig 4.17

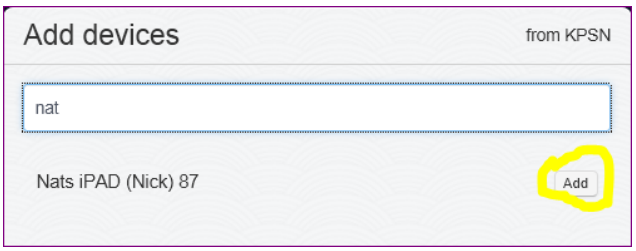


Fig 4.18

Enter the Device name of the desired Device and if it’s recognised as a valid device it will appear below the Search box (Fig 4.18).

Select Add (circled Fig 4.18) against the Device that you wish to Assign to the Group, it will change to Added when done (Fig 4.19).

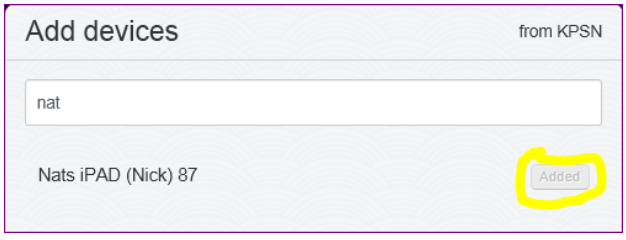


Fig 4.19

The Device would now appear within that Group (as in the example Fig 4.20).

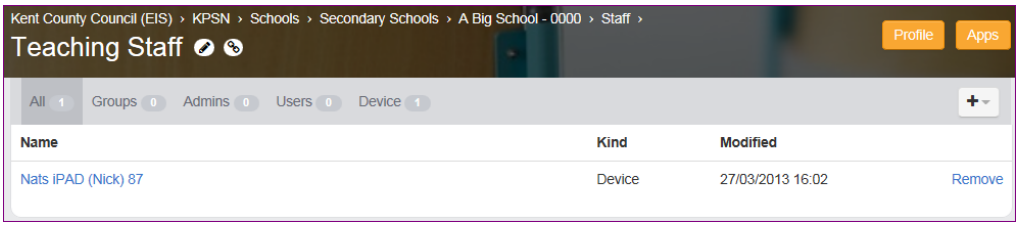


Fig 4.20

Remove Device from a Group

To Remove a Device from a Group you will need to navigate to the Group you wish to remove the Device from and then select Remove next to their Device instance, i.e.

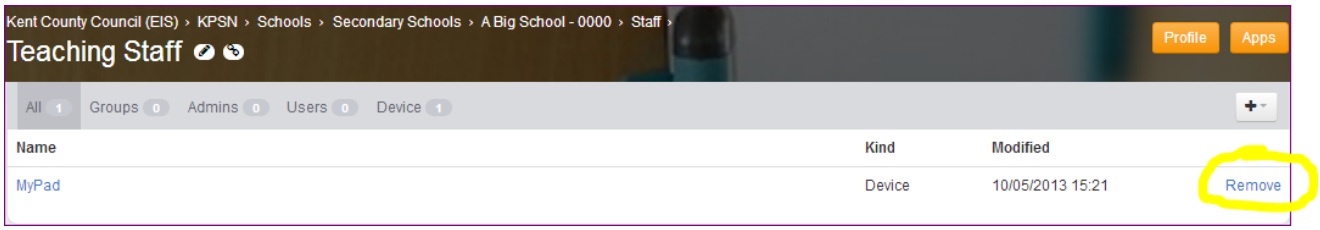


Fig 4.21

The above Device would be removed from the Group “Teaching Staff”.

Important Note: - If you remove a Device from MDM as above then currently you would have to re-enrol that Device into another Group when required for MDM Management. An alternative action could be that instead of Removing a Device that you create a “Holding Group” for unassigned Devices instead and simply move the unrequired device into the “Holding Group” until it’s required in a specific Group. This would ensure that the Device remains in MDM management at all times instead.

Assign a Device to a User.

To assign a Device to an existing User you should navigate to the intended User, Select the User and then from the Properties page select Actions (circled Fig 4.22).

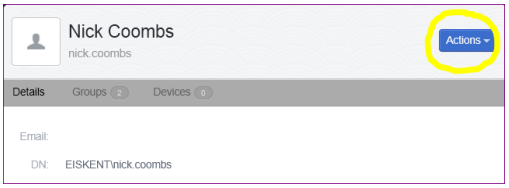


Fig 4.22

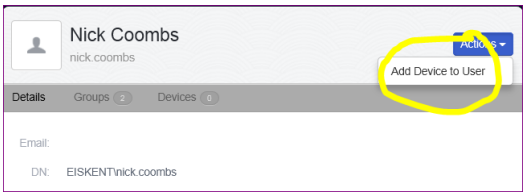


Fig 4.23

Then from the drop down box select Add Device (circled Fig 4.23).

Enter the Device name of the desired Device and if it's recognised as a valid device it will appear in the selection area (Fig 4.24).

Fig 4.24

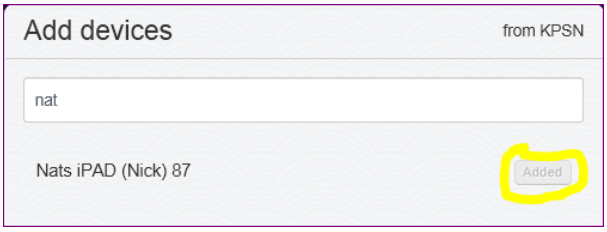


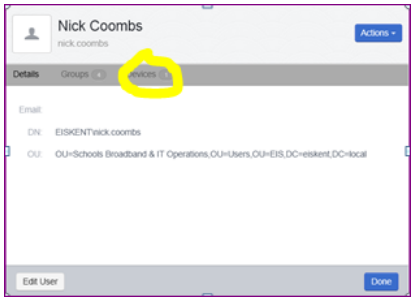
Fig 4.25

Select Add (circled Fig 4.24) against the Device that you wish to Assign to the Group, it will change to Added (Fig 4.25) when done.

The Device would now appear against that User when viewing the User properties page (See Users for further information).

Remove Device from a User

To Remove a Device from a User you will need to navigate to the User that you wish to remove the Device from and then select the User.



From the User Properties page select Devices (Fig 4.26).

Fig 4.26

And then select "Remove this Device from …" (circled Fig 4.27).

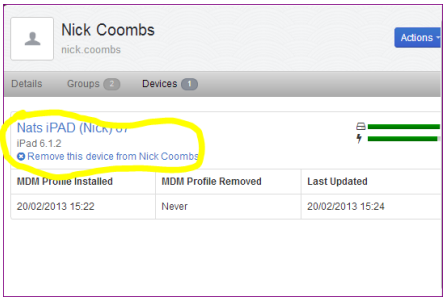
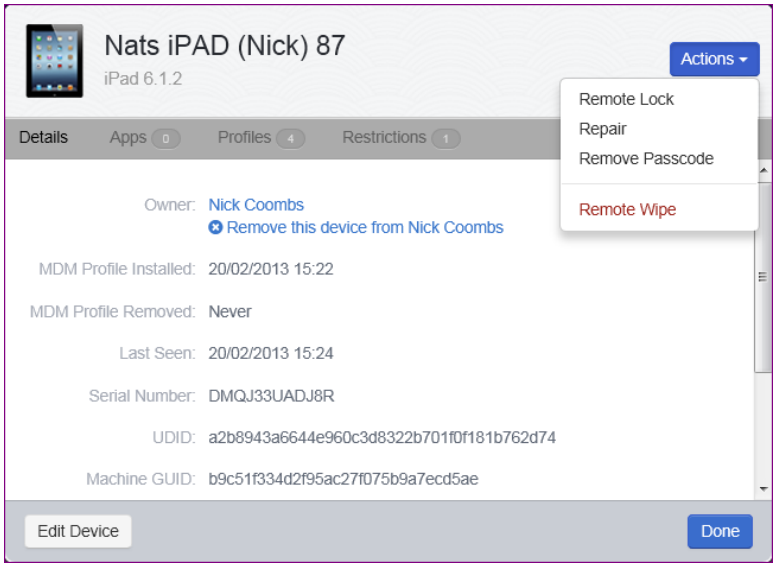


Fig 4.27

Device Property Page

The Device property page (Fig 4.28) illustrates information relating to the device, such as if its assigned to a User, its serial number, MDM profile status, profiles applied, installed Apps or Restrictions.



Selecting Actions reveals a dropdown where you can select a number of options.

Fig 4.28

Remote Lock a Device

Select Remote Lock to set the device to lock itself remotely, this will then require the Passcode to be used to return to the desktop.

Repair a Device

Select Repair to reinstall the applied profiles and Apps if it's suspected that anything is corrupted or if a user declined to install an App and doesn't wish to wait until the next auto retry from MDM.

Remove Passcode from Device

Select this option to remove a passcode from this device remotely.

Remote Wipe a Device

Select this option to remotely wipe a device and return it to factory defaults. This means it will be returned to a "just out of the box" state and so will no longer be in MDM.

MDM PROFILES

Profiles apply to Groups, Users and Devices. From within your Profiles you can configure how the device operates, its functions (known as Restrictions in Apple speak) and configurable items (such as email, calendars, Webclips) which are then inherited automatically as the profile applies to the device.

On the device itself you will potentially see a number of profiles (on an iOS device you will find these in “Settings > General”). You may see a “Supervised” profile, a “Mobile Device Management” and a profile for the membership Group that the device belongs to in MDM.

The Supervised profile means that the device is in Supervised mode with Mobile Device Manager to indicate that the device is Enrolled within MDM management. If you see that there is no Group profile on a device but there is a “Supervised” and a “Mobile Device Management” profile then it would mean that the device is currently not a member of a Group.

To view the Profile of a selected Group click on **Profile**

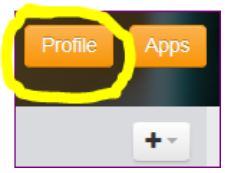


Fig 5.01

This reveals:-

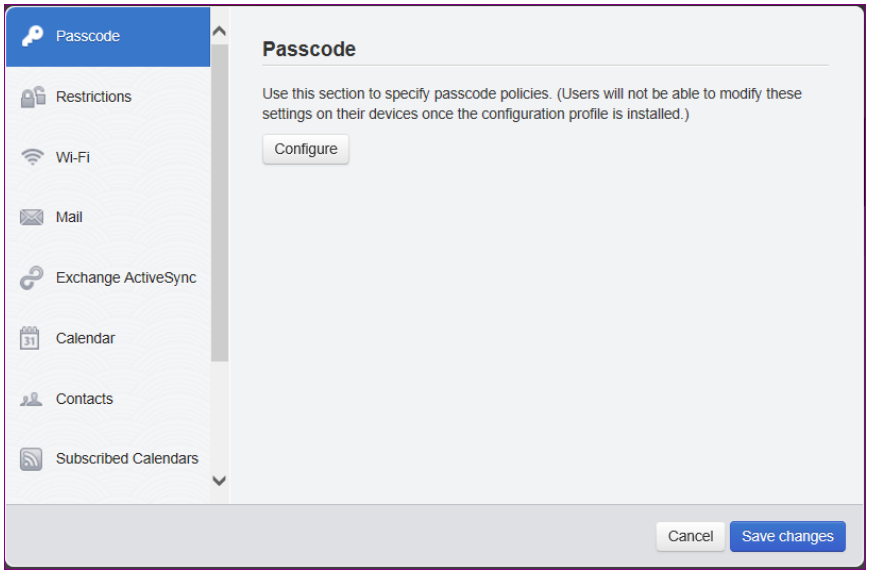


Fig 5.02

From here you can build your Group Profiles.

Profile Navigation

-/+ - In the Top right corner of each section you will notice -/+ paddles, use these to add or remove alternate variations.

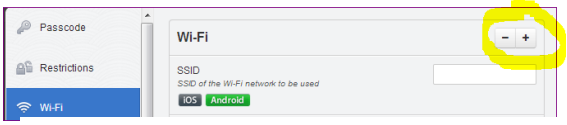


Fig 5.03

Inherited - This appears if the Restriction is Inherited from an upper Group level (Can be useful in troubleshooting).

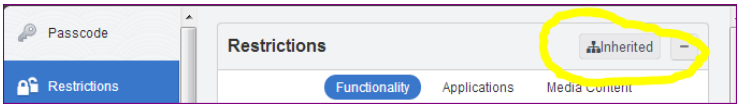


Fig 5.04

Profile Variables

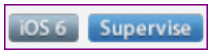
Profile Variables are popular fields from your schools AD that you may initially set in a profile much like a template. Then, if you use the "Authenticated Users" option for assigning your devices then these fields will be populated accordingly. Using this method it allows you to preconfigure configurable items such as email to then be personalised to the assigned user once they have Authenticated.

Variable	Definition
Device Variables	
%build_version%	The alphanumeric OS version installed on the device.
%device_name%	The name of the device.
%imei%	The International Mobile Equipment Identity serial number of the device.
%model_name%	The model name of the device.
%model_number%	The model number of the device.
%os_version%	The commonly-used OS version of the device.
User Variables	
%dn%	The user's domain name (domainname\username).
%email%	The user's email address.
%first_name%	The user's first name.
%full_name%	The user's full name.
%last_name%	The user's last name.
%ou%	The user's organization unit.
%user_name%	The user's user name.
%user_enrollment_url%	The user's web clip enrollment URL.

Fig 5.05

Variables can be used in any text field. For example, if you enter *%email%* in the Mail or Exchange ActiveSync Email Address field it would automatically populate on Authenticated Enrolment with the Users email address. If required you may use combinations of fields and join them to make longer strings, such as *%first_name%*.%last_name% (for firstname.lastname or (john.smith).

Explanation of settings that may then be managed through MDM.

Note: Options with 

can only be managed if the device has been supervised

Passcode - Use this setting to require a Passcode to be entered on the device in to order to unlock it. Other settings in here provide options to control the complexity of the code to match your schools security policies.

Restrictions - Use this setting to manage functionality on the device, such as whether the camera is enabled, use of iMessage, install of Apps etc.

Wi-Fi - Use this setting to manage or configure Wireless network profiles on your device. This will provide you access to SSID, WLAN behaviours, Proxy settings and Authentication parameters.

Mail - Use this option to configure your mail settings on the device using IMAP (Default) or POP.

Exchange ActiveSync - Use this option to configure your device to sync with an Exchange Server.

Calendar - Use this option to configure your device to sync to a CalDAV server (typically useful for organisation Calendars).

Contacts - Use this option to configure your device to sync to a CardDAV server (typically useful for organisation contacts).

Subscribed Calendars - Use this option to configure your device to subscribe to calendars (typically useful for non-organisation calendars, such as a UK Bank Holiday calendar).

Web Clips - Use this option to create URL shortcuts for your device desktop, these shortcuts could be to your schools website or other popular webpages.

Global Proxy - Use this option to configure the device to use a HTTP Proxy server for Internet Content Filtering when device is offsite on a non-school internet connection. Please contact the ServiceDesk if you wish to use this function.

App Lock - Use this to restrict the device to a single running App which has previously been deployed via MDM. This will also disable the “Home” button and Resume into the designated App after a Wake or Reboot event. Simply select the App from the Application Dropdown box.

 © EiS Kent

MDM APPS

MDM enables you to manage App deployments on your devices, to view your App Inventory, upload new Apps from iTunes with your VPP codes etc.

As you Add and Remove Apps to populated Groups they are normally committed in real time however, sometimes this could be several minutes or more during busy periods as the tasks join a queue.

Important to note: - If you have large Apps or many Apps that are to be deployed to many devices at once then you may wish to consider performing the deployments outside your schools peak times. This is because each App will be downloaded from the Internet using your schools internet connection to each device which may require high levels of bandwidth be available during the deployment.

View School Level Apps

To view all Apps in your school click on **Apps** from the School Bar.

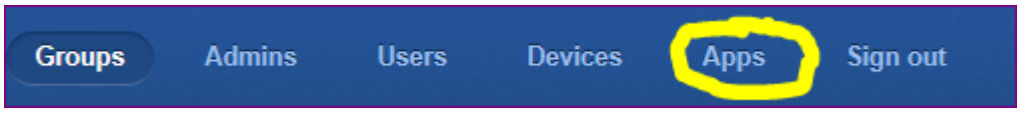


Fig 6.01

This then lists all the Apps with some useful info.

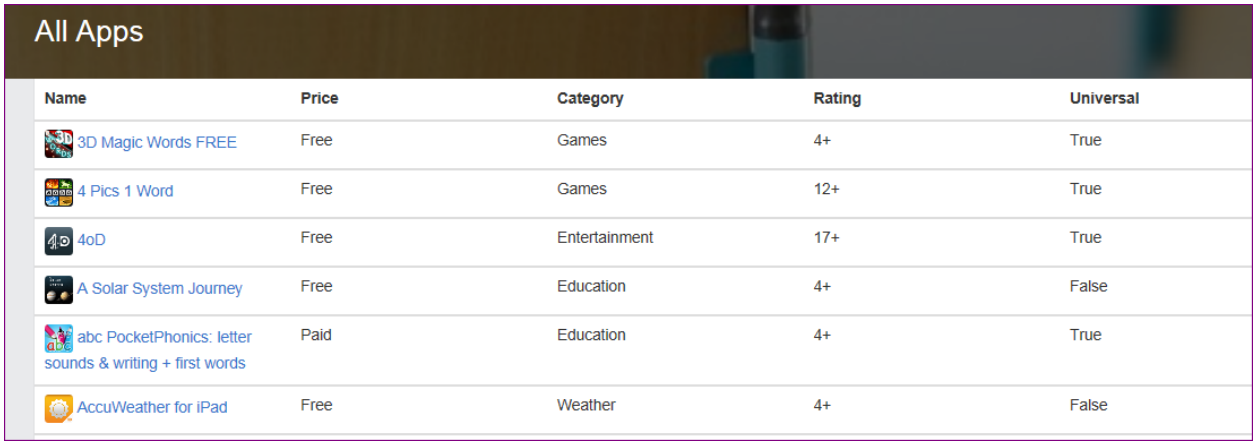


Fig 6.02

Select an App to view further information on it such as size, age rating, cost, a fuller description, version etc.

From within this further information view of the App you will also be able to view which Groups it exists within your school.

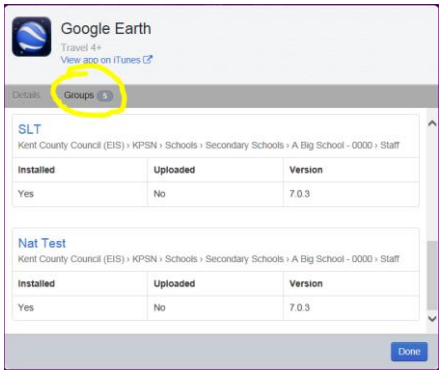


Fig 6.03

View Group level Apps

To view all Apps in a selected Group click on **Apps**.

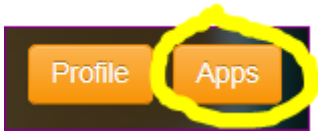
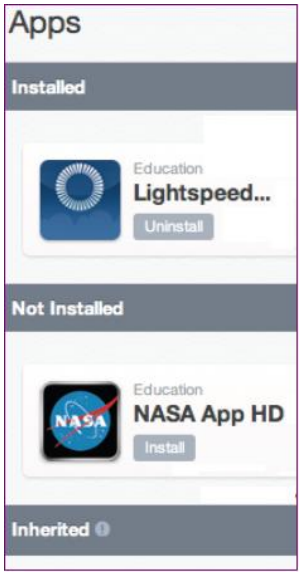


Fig 6.04

This will reveal options to install an App to the Group either from the online App Store or Upload an App from your computer (Previously downloaded from iTunes using your schools account).



You will also be able to see which Apps apply to the device (Installed, Uninstalled or Inherited).

Fig 6.05

Other options or information obtained from this screen are:

Reinstall App: - Use this to reinstall the App to the Group devices.

Uninstall App: - This will uninstall the App from the devices belonging to the Group.

Delete App: - This removes the App from Group availability and the Device itself.

Reinstall All: - Use this to reinstall all Group Apps to your Group devices.

Install an App

To install a new App to your Group select “Install an App” from the selected Groups Apps button;

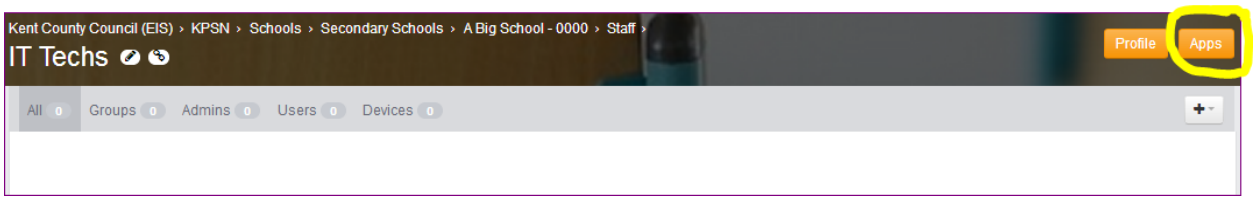


Fig 6.06

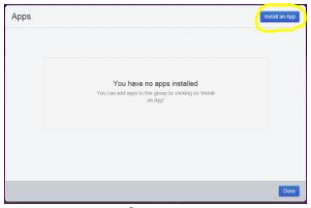


Fig 6.07

> > which takes you to install an App >>

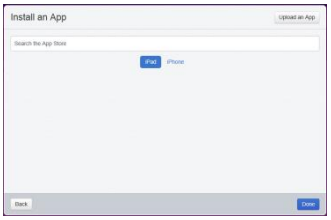


Fig 6.08

To install an App from MDM using live access to the App store please refer to “Web App Install” below.

To install an App from your PC or Mac iTunes please refer to “iTune App Install” below.

Web App Install

Note: - Depending on your Apple Deployment Model your devices may ask for credentials at the point of install. Its anticipated that most schools will use the “iTune App Install” method so that they may utilise their Schools Corporate iTunes account and deploy apps transparently (requiring no credentials being entered). Please refer to the section on “Apple Information” for further information on Apple Deployment options.

Free Apps

To install an App from the Web portal you can enter its name or search phrase within the “Search the App Store” search box.

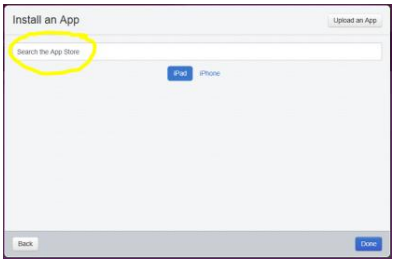


Fig 6.09

In the example on the right I have searched for “Goog” in order to locate “Google Earth”

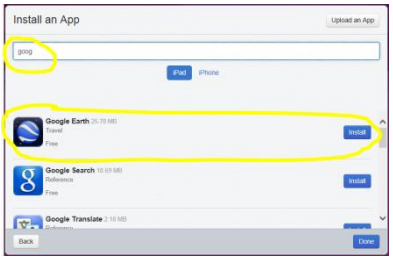


Fig 6.10

Once you have located the App that you require you can click on **Install** for it to be loaded from the App Store to your selected Group.

Pre-Paid Apps

Note: - To use this option you must have completed your schools acquisition of an “Apple Volume Purchasing Plan” (VPP), please read “Apple Information” for further information.

To install an App from the Web portal you can enter its name or search phrase within the “Search the App Store” search box.

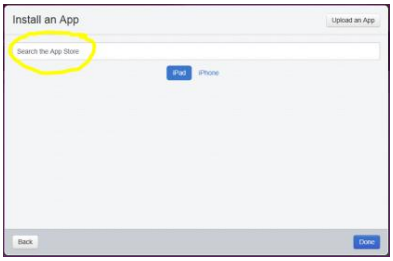


Fig 6.11

In the example on the right I have searched for “pages” in order to locate “Pages”.

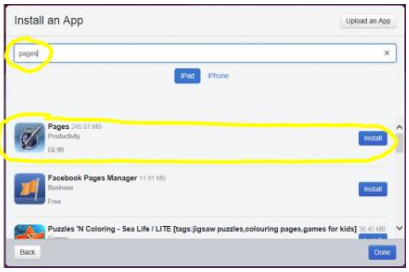


Fig 6.12

Once you have located the App that you require you can click on Install, as this is a Paid App it will prompt you as below:

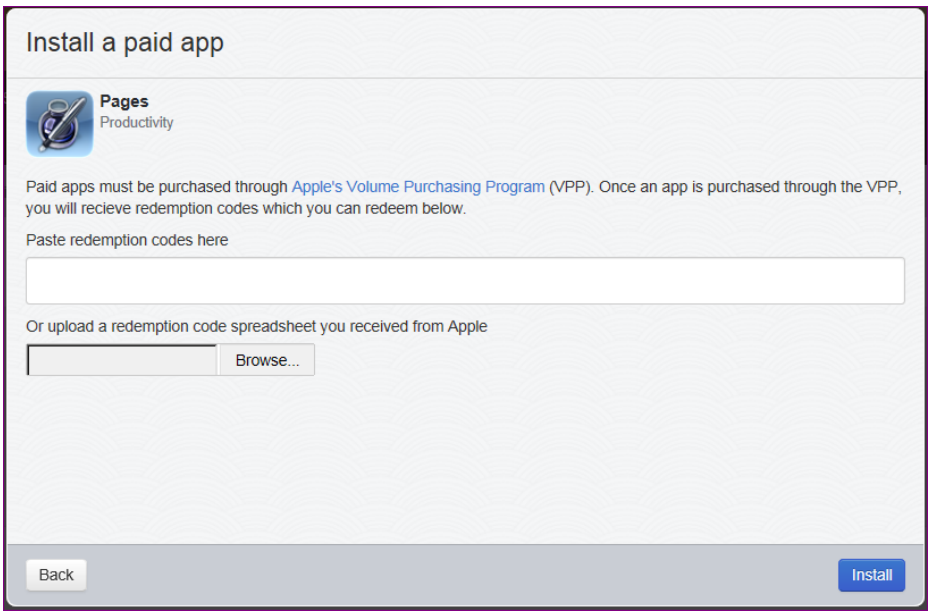

Install a paid app
Pages
Productivity
Paid apps must be purchased through Apple's Volume Purchasing Program (VPP). Once an app is purchased through the VPP, you will recieve redemption codes which you can redeem below.
Paste redemption codes here
Or upload a redemption code spreadsheet you received from Apple
Browse...
Back
Install

Fig 6.13

From here you may either enter the VPP code that you have received from Apple OR select “Choose File” to upload your Apple VPP spreadsheet. (Please refer to “My Apple VPP speadsheet” for further information).

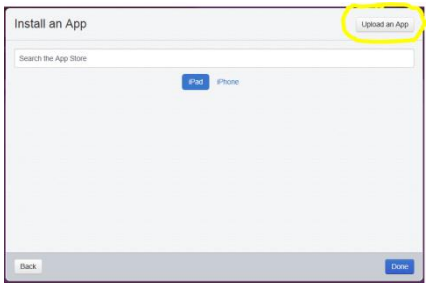
Once you have selected the applicable method of redemption select I**nstall** for the App to be deployed to devices within the selected Group.

iTune App Install

Note: - Use of this method is encouraged over the Web Install although its appreciated that it may be considered more complicated at first.

It requires you to have iTunes installed on your Designated Administrators workstation and recommends that you have access to your schools Corporate iTunes account (also known as Apple ID) that was used in your devices original setup and that your school has acquired their "Apple Volume Purchasing Plan" (VPP) (please read "Apple Information" for further information.)

If you have not set your devices up to use a single Corporate iTunes account (by assigning your schools Corporate iTunes account to the device on initial setup in Apple Configurator) then you will not be able to use a transparent App Deployment (requiring no credentials being entered).



Select "Upload an App" from the "Install an App screen.

Fig 6.14

This takes you to the next screen.

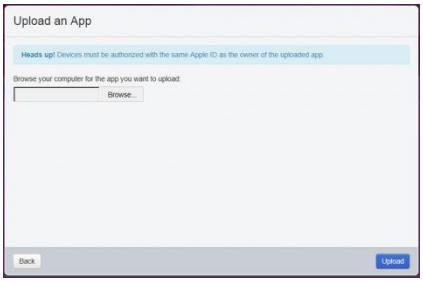
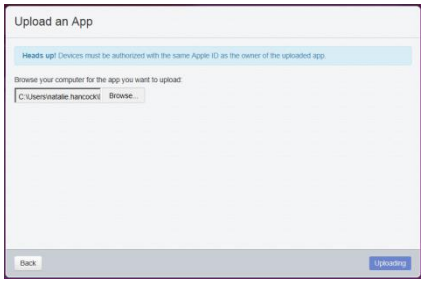

Upload an App
Heads up! Devices must be authorized with the same Apple ID as the owner of the uploaded app.
Browse your computer for the app you want to upload:
Browse...
Back
Upload

Fig 6.15

Select *"Browse"* to navigate to the location of your download store on your Designated Administrators workstation and select the IPA file for the App that you require then select *"Upload".*


Upload an App
Heads up! Devices must be authorized with the same Apple ID as the owner of the uploaded app.
Browse your computer for the app you want to upload:
C:\Users\natalie.hancock\
Browse...
Back
Uploading

The screen will change to reflect that an upload is taking place.

Fig 6.16

And will report that it has succeeded once completed. Click Done when finished. If using the transparent App Deployment method then Devices will now be prompted to install the App and will only need to click OK for it to install.

ENROLMENT

Enrolment is the process whereby your mobile device elects to allow MDM Manager to manage its Functionality (such as Enabling/Disabling features such as Camera/iMessage/Facetime), configuration and App deployments centrally 'over the air'.

You may typically reach this process once you have designed your schools Group structure.

Important to note: - If you have large Apps that are to be deployed to many new devices following Enrolment then you may wish to consider performing the Enrolment process outside your schools peak times. This is because each App will be downloaded from the Internet using your schools internet connection to each device which may require high levels of bandwidth be available during the process.

There are two valid Enrolment options available, Individual Enrolment and Bulk Enrolment. Both have their own pro's and con's however, we would recommend that for any school owned device that you use the Bulk Enrolment method as that will allow you to place the device into Apple's Supervise Mode (which shall be discussed below).

Apple Configurator and Apple Supervise Mode

Apple Configurator is Apple's default method of providing an organisation the ability to manage mobile Apple devices, principally as of writing, iPods, iPhones and iPads .

Apple Configurator requires that you have access to an Apple Mac with Apple Configurator downloaded from their software library. Once installed you can then organise your devices, name them, configure them and manage some features however, unlike with MDM, Apple Configurator can only manage devices that are directly connected to the Apple Mac via USB cables and only 30 devices at a time. MDM on the other hand, will allow management of the devices using wireless and to any number of devices that an organisation may own.

Apple Supervise Mode is Apple's elevated control method of limiting who may manage certain features on the IOS device, (much like Microsoft's User Access Control (UAC) in some versions of Windows). Functions that require Supervise level permissions in order for MDM to be able to manage them include Global Proxy (to provide content filtering to devices when not on the school network), iMessage, blocking of Erotica rated content in iBooks, permitting iBooks, allowing Removal of Apps etc.

All features and configurable options that require Supervise level permissions can be seen within MDM as they have Supervise next to them (i.e.

).

Important note: - If an iDevice is unSupervised then MDM will not be able to manage that level of feature on the device!

If you have iDevices already and wish to use the Supervise features of Apples IOS then you will need access to an Apple Mac and would need to download a copy of Apple Configurator before following the Bulk Enrolment method. If you have no way of configuring your devices into Supervise mode then please contact EiS who may be able to quote for assisting.

Important note :- Supervise mode can only be enabled during the initial setup using Apple Configurator, existing devices would need to be restored to default settings and content using Apple Configurator to enable Supervise mode.

Using Apple Configurator

This section discusses how best to prepare your devices for life within MDM and will demonstrate how to set them into Apple Supervise mode and ready to use your schools Corporate Apple ID (for use with either the Corporate or Layer Deployment models).

Create Template device

Open Apple Configurator with an initial device that you wish to configure connected via USB. This device will be used to create a very basic Apple Configurator template profile for you to base all your subsequent devices on.

Fig 7.01

Under **Prepare** (Settings) create a device name. At this stage you may wish to call it Default as it is only a temporary working file.

Set **Supervision** to **On** (This is important in order to use advanced IOS options and can only be done at this stage).

Select **"Create New Profile"** – Name the profile "Wi-Fi Settings" as this will be the wireless profile required for the devices to connect to your wireless once setup is complete, this is necessary so that MDM can automatically communicate to your devices for further management. If this is forgotten then once the device restarts it will be unable to access your network!

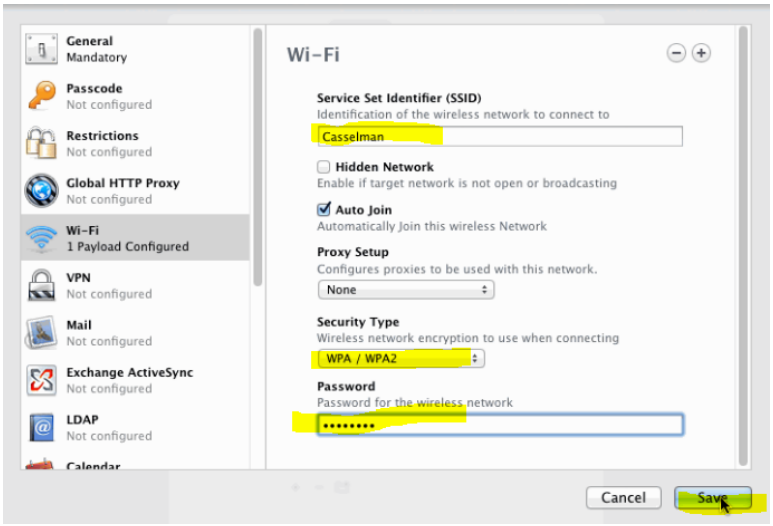


Fig 7.02

Configure the SSID, Security Type and Password.

Proxy Setup – This will be set to "None" for schools that use our Internet Content Filtering services however, if you use a 3rd party solution then enter their proxy information here.

Save the profile.

You will now have Wireless profile ready to apply to the device.

Select **Prepare** once you are ready for the profile to be assigned to the connected device. This will now completely erase the device so ensure if you had anything on here that you wished to keep that you had transferred it accordingly.

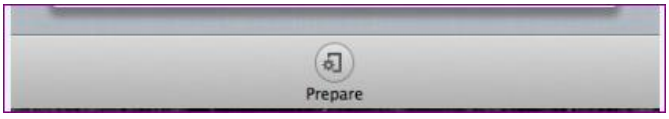


Fig 7.03

Once the device has been erased and set to Supervise Mode then you will see it appear as a Supervised item.

Fig 7.04

This will now allow you to complete the IOS Registration wizard on the device itself. You will need to set up Location Services, your Regional information, whether to use iCloud or not (It is suggested that with a Corporate Apple ID that you do not Enable this), Diagnostics etc.

Note: - When you are prompted for an Apple ID code you will need to enter your Schools Corporate Apple ID (see Apple ID/iTunes for further information)

Once the Registration Wizard is complete you may wish to tweak or adjust which settings are to be in which state (Enabled/Disabled), Homepage format etc. that should apply to all devices using this image.

Once you are happy with how your single device is configured then reconnect it to Apple Configurator and select Supervise.

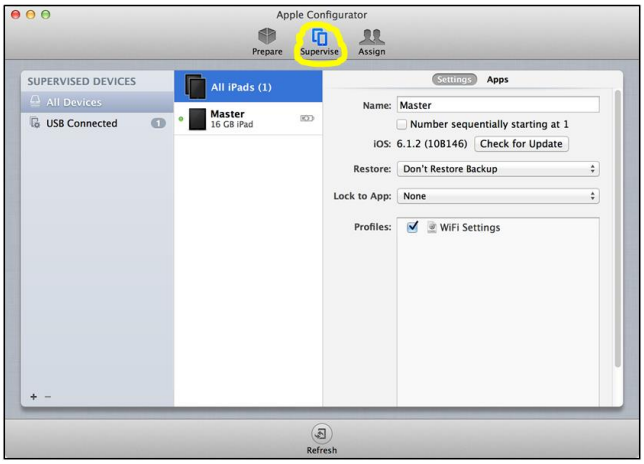


Fig 7.05

Ensuring that your original device name appears on the right next to Name, Right Click your mouse (or CTRL + Click if you do not have a two buttoned mouse) and select **Backup.**

You will then be asked for a Name of the Backup.

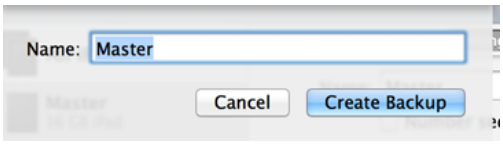


Fig 7.06

As this is now going to be your final working image file it is suggested to use something meaningful so that you may use the image in the future if you acquired additional devices. Further, you may need to have different base images for Staff and Student devices (different Home Pages, Event noises etc.) so name the file accordingly. Suggested convention would be your schools DfE's code plus Master followed by Staff/Student as necessary, i.e., "886-1111 Master" or "886-1111 Master Student". Once you have entered a suitable Name select Create Backup to continue.

Once the Backup is completed you are ready to proceed with Enrolment into MDM however, as the devices are currently in Supervise we need to remove this in order that the additional MDM profiles may be added.

Right Click the device in the current window and select Unsupervise, this will bring up a prompt asking you to confirm.

Unsupervise this device?
This will erase all content and settings on the selected device. Are you sure you want to do this?
Unsupervise Device
Cancel

Click **Unsupervise Device** to continue

Fig 7.07

This will cause the device to return to a Factory Default but do not worry; you saved all your template settings to the Backup image ready for the Enrolment process.

Device Enrolment

In Lightspeed MDM navigate to the Group that you require your device or devices to belong to. In the example below the group that is shown is called SLT (which is under "A Big School – 0000 > Staff").

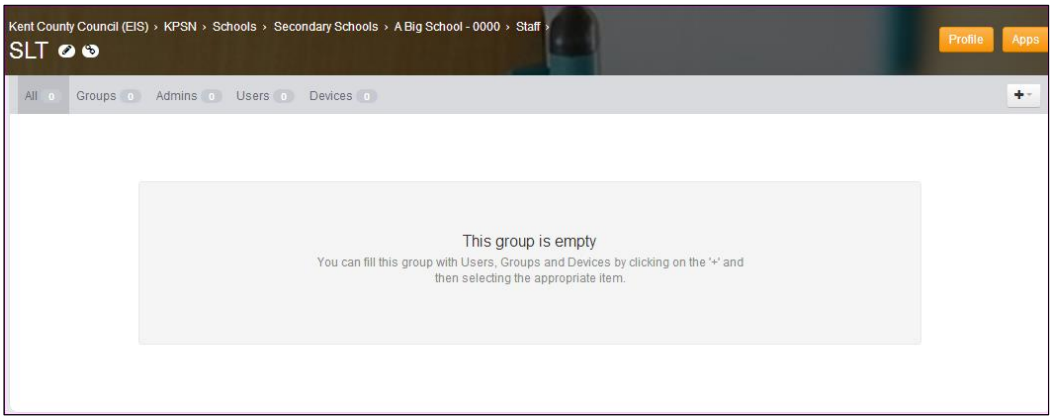

Kent County Council (EIS) › KPSN › Schools › Secondary Schools › A Big School - 0000 › Staff ›
SLT
Profile
Apps
All 0
Groups 0
Admins 0
Users 0
Devices 0
This group is empty
You can fill this group with Users, Groups and Devices by clicking on the '+' and then selecting the appropriate item.

Fig 7.08

Once you are in the desired Group then click on the link button, this is the icon second right (highlighted) to the Group name (Fig 7.09).

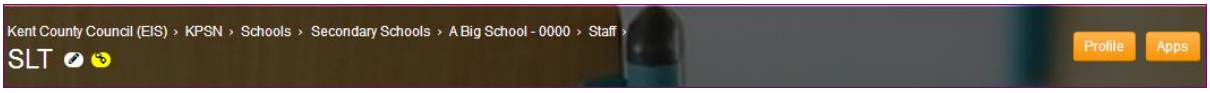


Fig 7.09

This will bring up the links for the Enrolment options available to you.

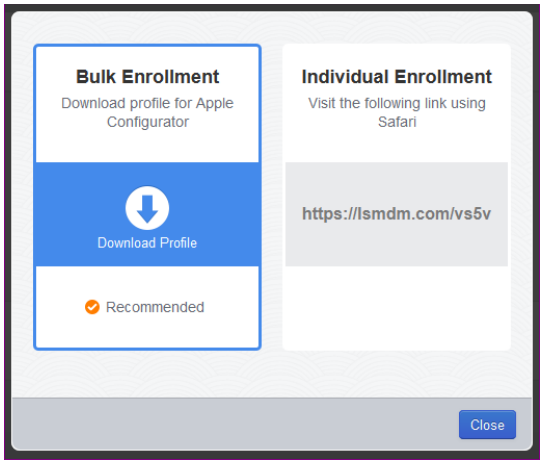


Fig 7.10

Bulk Enrolment allows you to download the Group profile information from MDM onto your Apple Mac for use in your Apple Configurator. Please follow the "Bulk Enrolment" section for further instructions in how to use this method.

Individual Enrolment provides you the URL that the intended client device should enter into Safari (or other browser) and then follows the "Individual Enrolment" section for instructions on how to use this method.

Bulk Enrolment

From the Enrolment Options box (see above Fig 7.10) select Download Profile and save it to an appropriate location on your Apple Mac.

Open Apple Configurator with the devices that you wish to configure connected via USB.

Fig 7.11

Under **Prepare** (Settings) create a device name, its advisable to use a meaningful naming convention as when you do MDM reports this is the name that you will see within the reports.

Suggested convention would be your schools DfE's code, i.e. "88#-####-Students" or "88#-####-Students-KS10". I.e., "886-1111-Students" or "886-1111-Students-KS10"

If you have more than one device to Enrol then tick "Number sequentially…" to auto-increment. Amend the starting number if you have used these numbers previously and wish to start higher up.

Set **Supervision** to **On** (This is important in order to use advanced IOS 6+ options and can only be done at this stage).

Set IOS to **Latest.**

Set **Restore** and navigate to the base template image you created for these devices.

Select **"Import Profile"** and select the profile that you downloaded from MDM earlier.

Select "Wi-Fi Settings" that you created previously.

If you are prompted with the following regarding Apps preservation then select Yes:-

Do you want to change Apple Configurator preferences to preserve apps and profiles it did not install?
With the current setting, apps and profiles installed by this MDM server will be removed when the devices are refreshed.
Do not ask me again
No
Yes

Fig 7.12

(If you select No then any Profile and Apps deployed by MDM will be removed if the device were to be reconnected to Apple Configurator in future).

Select **Prepare** when you are ready for the devices to start being imaged as per your base template device and Enrolled into MDM.

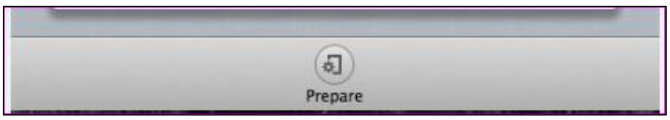


Fig 7.13

Once complete all further management will be able to be done in MDM as the devices will appear in the designated Group.

Individual Enrolment

This enrolment option is intended to be used when you have individual devices that you wish to be joined to Lightspeed MDM. These devices are likely to be un-Supervised and may be personal devices that require school Apps to be deployed, your schools AUPs may require devices to be in MDM, etc.

This method is an easy and straightforward way to add these types of Ad-hoc devices into your management.

On the Individual Enrolment option for the Group that you require you will see a URL (In the below example (Fig 7.14) it shows as https://lsmdm.com/vs5v).

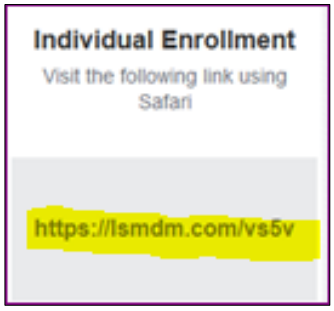


Fig 7.14

On the device that you wish to Enrol into Lightspeed MDM simply open a browser and navigate to the URL for the group that you require the device to be a member of.

This will initiate the install process by prompting a brief sequence of popups that need to be continued in order to complete.

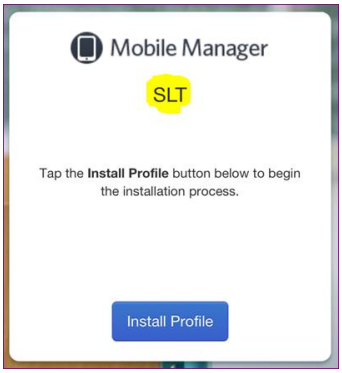


Fig 7.15

Destination membership Group highlighted (Fig 7.15, useful to verify it's the correct group).

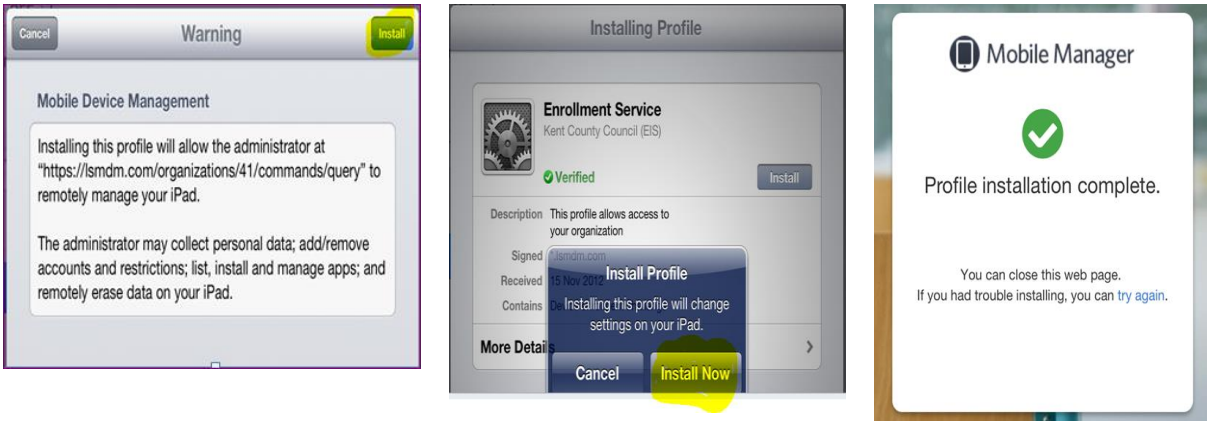

Cancel
Warning
Install
Mobile Device Management
Installing this profile will allow the administrator at "https://lsmdm.com/organizations/41/commands/query" to remotely manage your iPad.
The administrator may collect personal data; add/remove accounts and restrictions; list, install and manage apps; and remotely erase data on your iPad.
Installing Profile
Enrollment Service
Kent County Council (EIS)
Verified
Install
Description This profile allows access to your organization
Signed
Received
Contains
More Details
Install Profile
Installing this profile will change settings on your iPad.
Cancel
Install Now
Mobile Manager
Profile installation complete.
You can close this web page.
If you had trouble installing, you can try again.

Fig 7.16

And then…

The devices will now be in Lightspeed MDM and so all further configuration or management may be administered from there.

Advanced Enrolment options

As an extension of the two Enrolment methods you may wish to assign the Devices to your users so that they become Users within MDM, i.e., you will be able to manage the devices as a User (please see the chapter on Users for further information).

This method will require the user to first Authenticate themselves on the device prior to MDM assigning the device to them, this is because this is the only way currently that you may create a User instance from your schools AD into MDM.

This Authentication process populates the relevant information from your AD into MDM, once MDM recognises the User it can then use this information from your AD to populate bespoke configuration items and apply them per device (such as email configuration) which would be unique per person.

To use this feature you will need to be using our Lightspeed Next Gen filtering (if in doubt then please contact the Service Desk) and then to enable this Authentication requirement for a specific group you would need to amend or set the desired Group to “Authentication Required”. Once this has been enabled then any new devices joining that Group will prompt the user for their AD Username and password, once authenticated then any configuration fields set with variables will be populated accordingly.

Authenticating Devices to Users (Individual Enrolment)

To enable the Authentication requirement simply navigate to the Group that you require Authentication to apply (or create New Group).

Click on Group Properties.

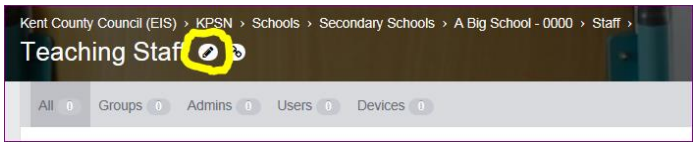

Kent County Council (EIS) › KPSN › Schools › Secondary Schools › A Big School - 0000 › Staff ›
Teaching Staff
All 0
Groups 0
Admins 0
Users 0
Devices 0

Fig 8.01

Then tick “Authentication required” (Fig 8.02).

Under **Tier** you will then need to ensure that your schools Tier is selected from the drop down.

Select **Update Group** to save and apply changes.

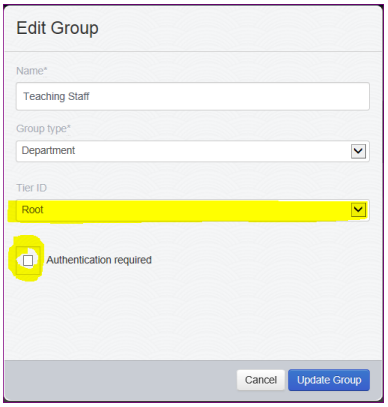


Fig 8.02

Remove the Tick if you wish to remove the Authentication requirement.

You will then need to create a Webclip to perform the Auto-population requirement of the data. For your selected Group select Profile then scroll down to Webclips (Fig 8.03).

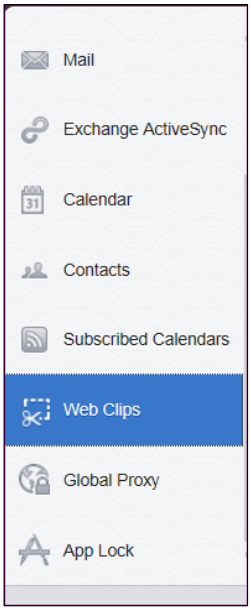


Fig 8.03

Then enter a Label name, i.e. “MDM Enrollment of Device” with URL of “%user_enrollment_url%”, (Fig 8.04).

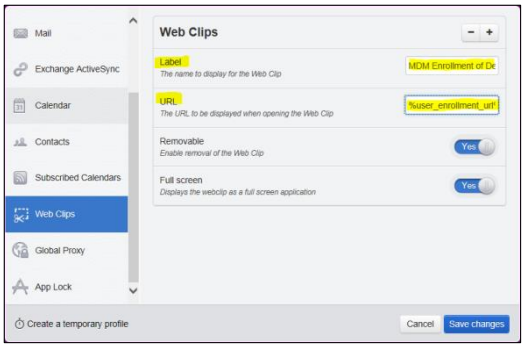


Fig 8.04

To then populate information from your AD to the User please review the chapter on “Profiles > Profile Variables”

APPLE INFORMATION

This section is designed to provide a brief overview to the help you navigate the initially confusing world of Apple terminology required to successfully implement an efficient and meaningful MDM environment. It is not intended to be a 'defacto' resource on all things Apple or to supersede their own information but is intended to point you in the right direction to complete some important steps.

Please ensure that you do read Apples information fully with regards to their legal requirements and your schools commitments to those legal obligations so that you satisfy any legal obligations expected of your school.

It is anticipated that schools will wish to be able to purchase Apps at discounted prices and so will be required to create an "Apple Education Volume Purchase programme" account profile. This purchasing account would then be used to acquire "Apple Redemption Codes" (also known as VPP code) or an "Apple Redemption Spreadsheet" for multiple purchases and these codes will be used through your schools Apple ID/iTunes account for deploying to the intended devices within MDM.

Apple Deployment Options

Apple currently has 3 App deployment models available and these are briefly discussed below together with a URL to Apples website for a video explanation.

Each model has its advantages for both deployment and ownership, the key relevance is for a school to decide how Apps are to be deployed and who are expected to be the App and content license "owner". The Deployment Model is relevant when you come to first register the iPads.

Institutional or Corporate Model

This model is anticipated to be the most widely used within our Kent school environments as typically the devices would be school owned and the only Apps expected to be deployed to the devices would by the Programme Facilitator. No one else is expected to install Apps.

The advantage of this model is that once the devices have been registered with the schools Apple ID then App deployment may be done transparently, meaning no credentials need to be entered and the school retain ownership of any Paid Apps or content (such as iBooks).

Go here for an overview: - http://www.apple.com/education/resources/videos/#ios-institutional-ownership

Personal Model

This model is unlikely to be used within schools as typically the devices are not likely to be school owned and/or each have their own Apple ID/iTunes account. This would mean that any Paid Apps or content (such as iBooks) are licensed by the iTunes account holder (which may not be the school).

You would not be able to use transparent deployment with this model, meaning that Apps deployed through MDM would require the device owner or user to enter valid Apple ID/iTune credentials to enable the install to take place.

Go here for an overview:
http://www.apple.com/education/resources/videos/includes/personal-deployment-model.html#personal-deployment-model

Layered Model

This model may potentially be seen in some schools, typically new academies (although not exclusively) where they utilise a 1-2-1 iPad deployment, meaning each student is provided a dedicated iPad.

This model would be used if the school expected to deploy Paid Apps and content (such as iBooks) that the school have paid for and wish to retain ownership of as the license owner, whilst also permitting the student to install their own Paid Apps purchased through the students own Apple ID/iTunes account.

Go here for an overview: - http://www.apple.com/education/resources/videos/includes/ios-layered-ownership.html#ios-layered-ownership

Apple Education Volume Purchase Programme

Apple has introduced a service for schools to bulk purchase Apps at a discount only available to Educational institutions. They require that the school first enrol into their programme and create a nominated Programme Manager and Programme Facilitator(s).

Programme Manager – This would typically be the Headteacher or Bursar. This person would be the legally responsible entity to Apple.

Programme Facilitator(s) – These would typically be your Designated Administrator, ICT staff, perhaps Heads of Departments (if you use Delegated Administrators in MDM). These accounts would be responsible for App purchasing and deploying them through MDM.

To sign up your school to the program please go to:
http://www.apple.com/uk/education/volume-purchase-program/

To read Apples FAQ please go to: http://www.apple.com/uk/education/volume-purchase-program/faq.html

To purchase from Apples Education store go to:
http://store.apple.com/uk/browse/home/education_routing

Once you have completed this then your Programme Facilitators will be able to Purchase Apps and obtain your schools VPP purchase codes or download your Apple Spreadsheet for uploading into MDM when deploying Paid Apps using the Web Install method.

You may find it useful to record your Programme Facilitator credentials on the MDM Reference Sheet at the back/bottom of this guide.

Apple ID/iTunes Accounts

In order to install Apps onto your schools iPads you will need to use an Apple ID, also known as an iTunes account. These accounts allow you to 'purchase' Apps and then install them onto the device.

In Apple terminology 'Purchase' is used to describe the elective action of proceeding with the acquisition of an App, irrespective of if any payment is made (Paid) or not (Free).

It is advised that a school create their free Apple ID/iTunes account and register their iPads using this one account (unless using the "Personal Model" for App deployment), this account can then be used in tandem with their Programme Facilitator account (for Paid purchases from the Apple Educational Volume Purchase Program) to manage their App deployments transparently (requiring no credentials be used for install).

Recommended account name would be to use a generic school account in order to protect from future difficulties should a specific individual of a named account leave. Suggested usernames could be itunes@myschool.kent.sch.uk (substitute "myschool" with your schools email domain address) but ensure that you have that account or alias configured so that it may receive emails.

To create your schools account or for more information please go to:
http://store.apple.com/uk/help/your_account

To download iTunes to your PC/Mac please go to:
http://www.apple.com/uk/support/itunes/

You may find it useful to record your schools Apple ID/iTunes credentials on the MDM Reference Sheet at the back/bottom of this guide.

MISCELLANEOUS INFORMATION

This section contains some suggested material to help tie all the previous sections together and so is written succinctly and on the strict assumption that you have read the earlier sections and so are familiar with the terminology used.

Where do I begin?

You have unpacked your mobile devices and are ready to begin but perhaps overwhelmed by all the earlier information! The below is a typical checklist or order to follow in order to end up with your devices in MDM. You may not start at Step 1, you may start and end somewhere in between and before the last step however, we hope it's a useful chronological resource.

- **Step 1 -** Create your schools Apple ID/iTunes account to use in a Corporate or Layered Deployment Model
- **Step 2 -** Create your schools Apple Education Volume Purchase Programme profile to purchase Paid Apps
- **Step 3 -** Apple Configurator – Supervise and create a Wireless Profile on initial device for initiating a template device image
- **Step 4 -** Manually setup/Register the template device with your schools Corporate Apple ID
- **Step 5 -** Apple Configurator – Backup the Registered Device from Step 4, template device image now created.
- **Step 6 -** MDM – Create your Group structure ready to Bulk Enrol devices into, download your Bulk Profiles
- **Step 7 -** Apple Configurator – Using applicable MDM Bulk Enrolment profiles perform Restore of template of Step 5 to applicable Devices
- **Step 8 -** Devices will now be in MDM, Supervised and able to use Corporate or Layered Deployments

 © EiS Kent

How Do I…?

Locate an App from iTunes on my Hard Drive

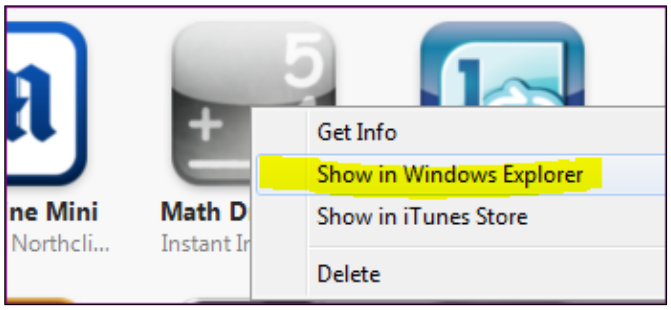
In order to use transparent deployment of Apps you will need to download them to iTunes on your PC/Mac using your School Corporate iTunes account, this will also apply for Paid Apps that you purchase through the schools Apple Education Volume Purchasing Programme.

You will then have the ipa files (the extension name for Apple Apps) ready to Upload into MDM when using the iTunes App Install method.

Locate your local App Store on your PC/MAC

Open iTunes and Right Click on an App that you are interested in:

Fig 9.01



Select “Show in Windows Explorer”.

Fig 9.02

This will bring up the source folder of your Apps in Windows Explorer.

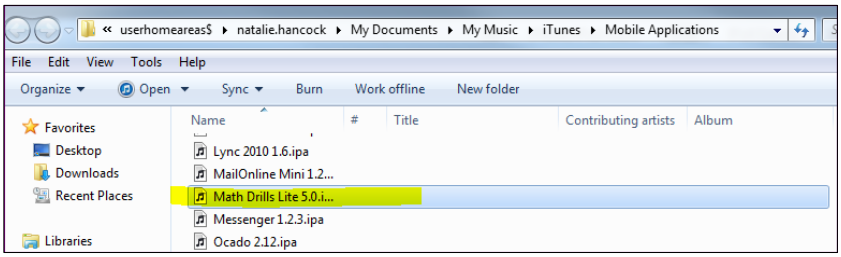


Fig 9.03

From here you could either, Left Click the mouse and drag (Copy) the files to a familiar location for uploading into MDM using the iTune Install method OR, simply remember the location so that you may navigate to it when prompted in MDM.

My Apple VPP spreadsheet

When you purchase Apps from Apple's Education Store using your Apple Education Volume Purchase Programme ID you have the option of downloading an Excel XLS spreadsheet. This Apple Spreadsheet contains all the VPP codes related to that App purchase which you may redeem within MDM using the Web Install method when deploying your Apps.

The below provides an overview of what you can expect to see however, Apple may change it from time to time to reflect their own evolving processes.

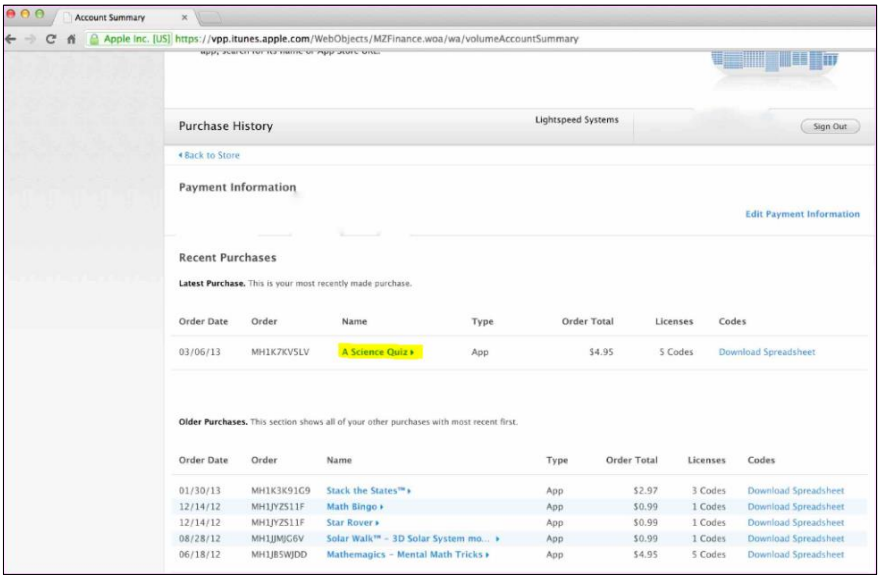
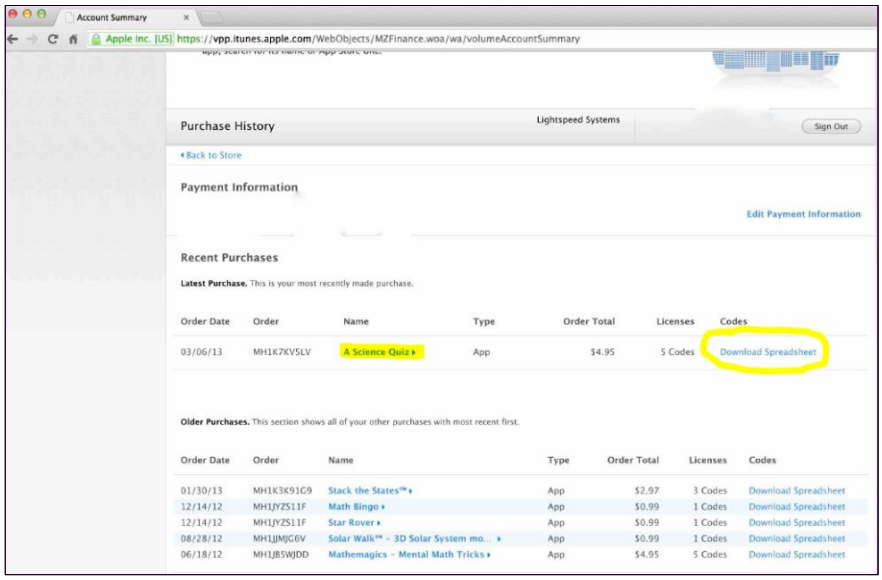

Account Summary
Apple Inc. [US] https://vpp.itunes.apple.com/WebObjects/MZFinance.woa/wa/volumeAccountSummary
Purchase History
Lightspeed Systems
Sign Out
Back to Store
Payment Information
Edit Payment Information
Recent Purchases
Latest Purchase. This is your most recently made purchase.
Order Date Order Name Type Order Total Licenses Codes
03/06/13 MH1K7KV5LV A Science Quiz App $4.95 5 Codes Download Spreadsheet
Older Purchases. This section shows all of your other purchases with most recent first.
Order Date Order Name Type Order Total Licenses Codes
01/30/13 MH1K3K91C9 Stack the States™ App $2.97 3 Codes Download Spreadsheet
12/14/12 MH1JYZS11F Math Bingo App $0.99 1 Codes Download Spreadsheet
12/14/12 MH1JYZS11F Star Rover App $0.99 1 Codes Download Spreadsheet
08/28/12 MH1JJMJG6V Solar Walk™ – 3D Solar System mo... App $0.99 1 Codes Download Spreadsheet
06/18/12 MH1JB5WJDD Mathemagics – Mental Math Tricks App $4.95 5 Codes Download Spreadsheet

Fig 9.04

Purchase your App of interest, in the example in Fig 9.04, its "A Science Quiz".

You will then be able to select "Download Spreadsheet" (circled Fig 9.05) to download to your PC/Mac.

Fig 9.05


Account Summary
Apple Inc. [US] https://vpp.itunes.apple.com/WebObjects/MZFinance.woa/wa/volumeAccountSummary
Purchase History
Lightspeed Systems
Sign Out
Back to Store
Payment Information
Edit Payment Information
Recent Purchases
Latest Purchase. This is your most recently made purchase.
Order Date Order Name Type Order Total Licenses Codes
03/06/13 MH1K7KV5LV A Science Quiz App $4.95 5 Codes Download Spreadsheet
Older Purchases. This section shows all of your other purchases with most recent first.
Order Date Order Name Type Order Total Licenses Codes
01/30/13 MH1K3K91C9 Stack the States™ App $2.97 3 Codes Download Spreadsheet
12/14/12 MH1JYZS11F Math Bingo App $0.99 1 Codes Download Spreadsheet
12/14/12 MH1JYZS11F Star Rover App $0.99 1 Codes Download Spreadsheet
08/28/12 MH1JJMJG6V Solar Walk™ – 3D Solar System mo... App $0.99 1 Codes Download Spreadsheet
06/18/12 MH1JB5WJDD Mathemagics – Mental Math Tricks App $4.95 5 Codes Download Spreadsheet

For info, if you were to open the XLS file it would appear something like:

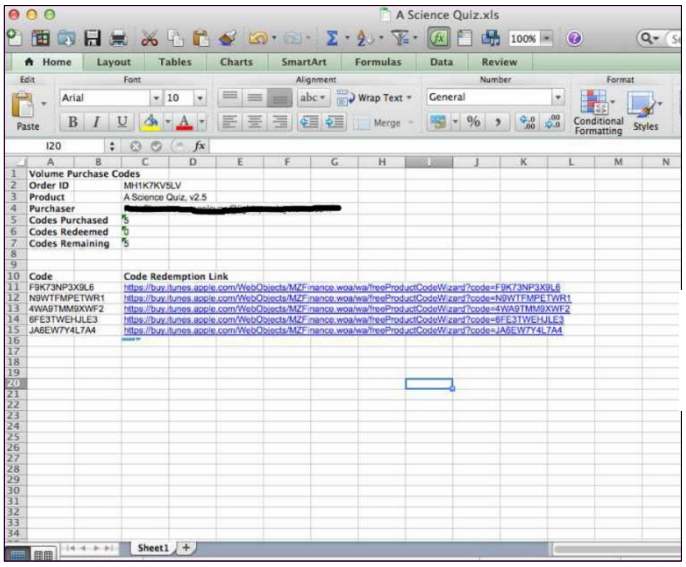
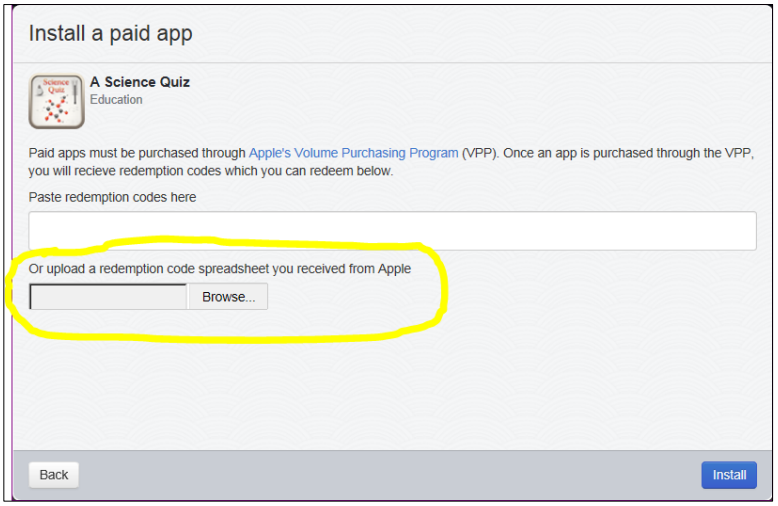


Fig 9.06

When later deploying an App using the Web Install method and you are prompted for the "…redemption code spreadsheet…" (As in Fig 9.07) you may select Browse and then navigate to your downloaded spreadsheet for that App.

Fig 9.07


Install a paid app
A Science Quiz
Education
Paid apps must be purchased through Apple's Volume Purchasing Program (VPP). Once an app is purchased through the VPP, you will recieve redemption codes which you can redeem below.
Paste redemption codes here
Or upload a redemption code spreadsheet you received from Apple
Browse...
Back
Install

TROUBLESHOOTING

In the event that you do require any assistance with MDM then please endeavour to check our online Frequently Asked Questions resource at www.eiskent.co.uk?faqmdm first.

This location will be regularly updated with the common questions and assistance articles to help you resolve any problems 24/7 in your own time however, if you do require further assistance then please contact the EiS ServiceDesk on 01622 672779 or via email at support@eis.kent.gov.uk or through your regular support channels.

This additional MDM Support MAY be chargeable depending on which support contracts you have in place.

 © EiS Kent

MDM REFERENCE SHEET

Your corporate Apple ID/iTunes account User / Password:

Your Apple Programme Facilitator ID User/Password:

Your MDM Administrator User/Password:

Our passion in EiS Kent is to make a real difference in education and ultimately children's lives by providing innovative solutions and outstanding support services.

www.eiskent.co.uk
info@eis.kent.gov.uk

Tel: 0300 065 8888
Fax: 01622 663591

EiS Kent
The Shepway Centre
Oxford Road
Maidstone, Kent
ME15 8AW

05.2013/MDM/UserGuide/V1/NH